# UNIVERSIDAD NACIONAL AUTONÓMA DE MÉXICO


**FACULTAD DE INGENIERÍA**

# SEGMENTACIÓN DE LA RED DE LA BIBLIOTECA CENTRAL DE LA UNAM

**TESIS**

**QUE PARA OBTENER EL TÍTULO DE:**

**INGENIERO EN COMPUTACIÓN**

**PRESENTA:**

**MARIO MAGDALENO BARRERA HERNÁNDEZ**

**DIRECTOR DE TESIS**

**M.I. MARCIAL CONTRERAS BARRERA**

**CIUDAD UNIVERSITARIA 2010**

**AGRADECIMIENTOS**

*Dedicado a mi familia y a todos los necios que me estuvieron molestando para que hiciera de una vez por todas esta tesis. Les doy las gracias a todos por el apoyo que me dieron durante las diferentes etapas de mi vida.*

*Mis padres, mis hermanos y todos mis sobrinos han sido motivo por el cual uno puede hacer un poco más del 100%, a pesar de todo…*

*A mi familia, mi Papá Gonzalo, mi Mamá Agueda, mis hermanos Agueda "nena", Lorena "petus", Jaime "cheja", mi cuñada Gaby y mi cuñado Raúl, mis sobrinos Roberto, Eric, Samantha, Diego, Liliana, Sofía, Víctor y los que vengan, todos son y serán parte de mi vida.*

*A mis compañeros de trabajo, Marcial Contreras Barrera, Arcadio Gamero Arenas, Gonzalo Reséndiz Cansino, Alberto Ramos, Angélica Briones, Verónica Vargas, Abraham Hernández Ramírez, Rodrigo Ramírez López, Israel Díaz Chavarría.*

*A los amigos y colegas, Amelia Pérez Islas, Filiberto García Solís, Jeannette Ramírez Pacheco, Don Manuel, Patricia Solano Martínez, María de los Ángeles Meza Barrera, Emma Ordoñez, Rosa Balcázar Gómez e Ivonne García Carmona.*

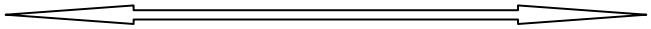
*Al médico Víctor Carmona Manzanares, por curar y atender a mi familia, y por ser uno de los necios.*

*Agradezco también a todos los demás amigos y compañeros que no enlisto, pero que siempre han estado o estuvieron presentes en algún momento para apoyarme.*

*Doy especial agradecimiento a Liz Marlene García Anaya, porque me mostró, desde el momento que la conocí, muchas cosas de manera directa e indirecta en las que no tenía ni visión ni toma de decisiones, las cuales influyeron para que decidiera tomar mi propio camino. Siempre estará presente en todos mis logros.*

*Dedicado a Dios por haberme dado más vida de la que me correspondía.*

*En la noche sombría*
*vuela un fantasma iridiscente.*
*Se eleva y despliega las alas*
*sobre la negra e infinita humanidad.*
*Todo el mundo lo invoca*
*y todo el mundo lo implora,*
*pero el fantasma desaparece*
*con la aurora*
*para renacer en el corazón.*
*¡Y cada noche nace,*
*y cada día muere!*



*¡Brilla como la llama*
*y no es llama!*
*Es tal vez delirio.*
*¡Es fiebre de ímpetu y ardor!*
*¡La inercia lo cambia*
*en languidez!*
*Si te pierdes o mueres se enfría.*
*Si sueñas la conquista,*
*¡se inflama, se inflama!*
*¡Tiene una voz,*
*que escuchas palpitante*
*y es el vivo resplandor del ocaso!*

*Turandot,* Giacomo Puccini

*En la aventura*
*confié el coraje*
*guardé esperanza*
*y tracé mi mapa…*
*Un recorrido a*
*la altura del tesoro*
*descifrable sólo*
*por su brújula*
*e invariable al*
*caer arena de*
*su reloj…*

Jacqueline Aguilera

Pág.

## Capítulo 1. Antecedentes



## Capítulo 2. Teoría de redes

Pág.



## Capítulo 3. Redes Ethernet

Pág.

## Capítulo 4. Análisis y diseño



## Capítulo 5. Implementación, pruebas y mantenimiento

# Imágenes

Pág.

# Tablas

# CAPÍTULO 1

# ANTECEDENTES

## 1.1 Introducción

En 1950 se inició la construcción del inmueble que, en un principio, estaba destinado a la Biblioteca y Hemeroteca Nacional, pero por problemas burocráticos no prosperó dicho proyecto; por lo tanto, se decidió fundar otra. Así surgió la Biblioteca Central (BC) de la UNAM, la cual se pensó para controlar el sistema bibliotecario de la entidad y ofrecer un servicio adecuado para la consulta de información de los usuarios que llegaran.

El 5 de abril de 1956, la Biblioteca Central abre sus puertas a la comunidad universitaria. Estaba organizada sólo por cuatro departamentos: Publicaciones periódicas, Préstamo, Consulta y Reserva. En ese entonces, el servicio se ofrecía mediante la modalidad de estantería cerrada, y los usuarios debían llenar papeletas para solicitar un libro para consulta interna o préstamo a domicilio. Este procedimiento era lento, debido a que el encargado tenía que ir personalmente a buscar el libro en el estante correspondiente al piso donde se ubicara el material.

En 1966, se crea la Dirección General de Bibliotecas (DGB), encargada de la coordinación del sistema bibliotecario de la UNAM, cuyos objetivos principales son el apoyo a la docencia y la difusión del conocimiento y la cultura.

Los primeros acercamientos entre la tecnología y la DGB ocurren en el año de 1973, cuando se sustituyeron las fichas bibliográficas por un banco de datos que empleaba dispositivos magnéticos para su almacenamiento. Esto resultó ser muy útil para el usuario, pues podía ubicar el ejemplar buscado fácilmente. Esta base de datos se ubicaba en el Instituto de Investigaciones en Matemáticas Aplicadas y en Sistemas (IIMAS), y fue el primer paso para generar las bases de datos que se utilizan actualmente.

En 1975, al consolidarse como una entidad administrativa debido a las labores especializadas que el personal empezaba a realizar, se requirieron nuevos recursos, tanto humanos como tecnológicos, por lo que hubo la necesidad de comunicarse con la computadora central que utilizaba el PUC (Programa Universitario de Cómputo).

En 1976, se generó el sistema de procesamiento y recuperación bibliográfica LIBRUNAM, que fue elaborado en ALGOL (Algorithmic Language).

En el año de 1980, se inicia el servicio de estantería abierta donde el usuario pudo tener acceso directo al acervo.

En 1985, se adquirió un equipo para el manejo de bases de datos relacionales, llamado IDM (Intelligent Database Machine) y dos equipos Alpha Micro, en los cuales se implementa LIBRUNAM. Posteriormente, debido al éxito alcanzado se generaron nuevas bases como SERIUNAM, CIRCULA y TESIUNAM.

En los años subsecuentes, se agregaron mejoras en las bases y en la comunicación, pero un gran cambio significativo ocurrió para el año de 1994, en el cual se terminó de implementar la primera red LAN (Local Area Network: Red de Área Local) de la DGB, la cual quedó constituida de la siguiente manera:

- 184 nodos en red
- 10 concentradores cabletron de 12 puertos
- 2 concentradores cabletron de 24 puertos
- 1 puente
- Topología definida en estrella
- Equipos personales con D.O.S. de Microsoft
- Equipos personales con Windows 3.1
- Entrega de un segmento de red el 132.248.67.0 por parte de la DGSCA (Dirección General de Servicios de Cómputo Académico)
- 4 Servidores SunSparc con una base principal dedicada cada uno. LIBRUNAM, TESIUNAM, SERIUNAM y base de datos OPAC, manejando S.O. UNIX y Circula para BC
- Instalación de cableado UTP categoría 3 y 4
- Velocidad de transmisión 10Mbps semidúplex

Aunado a esto, se implementó el servicio de catálogo electrónico en 36 computadoras, las cuales tenían la información bibliográfica en CD-R o en el disco duro, pero el inconveniente de este método es que se tenía un retraso de disponibilidad de información en estos medios de, por lo menos, un año respecto al acervo real en la base de datos, debido a la realización de estos CD-R, tiempo de entrega e implementación.

En el año de 1997 se dio otro cambio importante, debido a que se adquirió el sistema gestor de bibliotecas Aleph, versión 300, mediante el cual se automatizó el procedimiento de adquisición, catalogación y préstamo del material bibliográfico.

En el año 2000, se implementa el cableado estructurado bajo el concepto de IDF (Intermediate Distribution Frame) y MDF (Main Distribution Frame).

En el año de 2003, se renueva el área de consulta especializada de información.

En el periodo de 2004, debido al incremento de servicios y proyectos futuros en los cuales se requería acceso a la red de la DGB, la Subdirección de Informática se enfrentó a graves problemas de saturación en el ancho de banda, disponibilidad de nodos y direcciones IP. Se cambió el ancho de banda de 10Mbps a 100Mbps ese mismo año.

Para resolver el problema de disponibilidad de nodos, se empezó la realización de cableado estructurado, mediante la contratación de empresas como KNEOS TCE, S.A. de C.V., y NST, México, S.A. de C.V.; ambos instalaron 450 nodos únicamente en dos niveles de la biblioteca. Después de terminados los contratos con las dos referidas empresas, la Subdirección de Informática decide que las subsecuentes instalaciones de cableado estructurado las realizaría personal del departamento de Producción de la misma Subdirección de Informática de la DGB.

A partir de 2005, se inician las actividades de canalización y cableado categoría 6 en diferentes pisos de la Biblioteca Central. En este año está por terminarse el proyecto de cableado.

En el año de 2006, se inauguran las salas de videoconferencia y se cambia la acometida de RedUNAM a 1Gbps.

En 2007, la DGB participa en el proyecto RIU (Red Inalámbrica Universitaria) de la DGSCA en CU mediante la utilización de redes inalámbricas y equipos portátiles.

Para darle solución a la disponibilidad de nodos, mientras se terminaba la parte del cableado estructurado para poder dar el acceso a la red, se aumentaron conexiones mediante switches no administrados o concentradores, colocados de manera tal que se pudiera dar servicio a la mayoría de los equipos que lo pidieran; en algunos casos se tenían que poner apilados. Esto ocasionaba caída en el rendimiento en el acceso a la red. Posteriormente, se redujo este problema con el avance del cableado estructurado.

Para la parte del direccionamiento IP, en un principio se implementó, por parte del Departamento de Producción, un servidor DHCP (Dynamic Host Control Protocol) basado en Windows NT para dar solución a la creciente demanda de acceso a red. En un principio fue aceptable, pero al poco tiempo empezó a tener caídas en el servicio, a causa de que las demandas de acceso por DHCP sobrepasaban la capacidad del equipo, o el equipo se degradaba debido a la misma demanda.

En consecuencia, se implementó un equipo en el Departamento de Consulta de la Biblioteca Central, mediante direcciones privadas pero estáticas de manera exclusiva para este departamento, mediante sistema operativo tipo Unix OpenBSD, y otro mediante el esquema DHCP dinámico para todos los demás departamentos, o equipos que no tuvieran IP’s físicas. Esto redujo de manera considerable las frecuentes reducciones de velocidad o problemas de acceso a red en el edificio. Aún así, era insuficiente el servicio, debido a que los servicios siguieron incrementándose como la RIU, videoconferencia, servicios de auto préstamo y verificación de salida de libros, sala de discapacitados, entre otros.

En la tabla 1.1, se muestra el crecimiento de nodos de red en la Biblioteca Central, en la cual nos podemos dar cuenta del incremento considerable de éstos, tomando en cuenta que en el cableado estructurado implementado en 2003 y 2009 se contemplaron tanto servicio de datos como servicio de voz.

| Piso | 1985 | 1996 | 2003 | Agosto 2009 | Área actual |
|---|---|---|---|---|---|
| Basamento | 22 | 24 | 68 | 68 | Producción |
| Basamento | -- | -- | -- | 2 | Imprenta |
| Basamento | -- | -- | -- | 2 | Restauración |
| Basamento | 16 | 24 | 55 | 55 | Procesos técnicos |
| Basamento | 10 | 12 | 42 | 42 | Adquisiciones |
| Basamento | -- | -- | -- | 28 | Sala de videoconferencia |
| Basamento | -- | -- | 50 | -- | Unidad administrativa |
| Basamento | -- | -- | 18 | 2 | Selección y adquisiciones |
| Planta principal | 8 | 12 | 12 | 12 | Préstamo |
| Planta principal | 18 | 24 | 24 | 32 | Catálogo electrónico |
| Planta principal | -- | -- | -- | 20 | Subdirección de BC |
| Planta principal | -- | -- | -- | 14 | Consulta |
| Planta principal | -- | -- | -- | 4 | Caja |
| Planta principal | -- | -- | -- | 4 | Auto préstamo |
| Planta principal | -- | -- | -- | 4 | Revisión de libros y accesos BC |
| Entrepiso | 14 | 16 | 16 | 39 | Sistemas |
| Entrepiso | 5 | 5 | 5 | 17 | Dirección |
| Entrepiso | -- | -- | 71 | 71 | Consulta |
| Planta alta | 10 | 12 | 12 | 62 | Planeación |
| Planta alta | | | | 52 | Secretaría académica |
| Piso 1 | 10 | 12 | 12 | 26 | Catálogo electrónico y préstamo |
| Piso 2 | 4 | 6 | 6 | 22 | Catálogo electrónico y préstamo |
| Piso 3 | 1 | 1 | 2 | 22 | Catálogo electrónico y préstamo |
| Piso 4 | 1 | 1 | 2 | 26 | Catálogo electrónico y préstamo |
| Piso 5 | 1 | 1 | 2 | 22 | Catálogo electrónico y préstamo |
| Piso 6 | 1 | 1 | 1 | 48 | Publicaciones periódicas |
| Piso 7 | 6 | 6 | 6 | 2 | Publicaciones periódicas |
| Piso 7 | | | | 2 | Fondo antiguo |
| Piso 8 | 3 | 3 | 3 | 80 | Tesis |
| Piso 9 | 4 | 4 | 4 | 28 | Desarrollo de personal |
| Piso 9 | | | | 32 | Catálogo colectivo |
| Piso 9 | | | | 24 | Publicaciones |
| Piso 9 | -- | -- | -- | 2 | Educación continua |
| Piso 10 | -- | -- | -- | 50 | Aula de capacitación |
| Piso 10 | -- | -- | -- | 28 | Fondo antiguo |

Tabla 1.1 Lista de nodos disponibles en diferentes periodos

## 1.2 Planteamiento del problema

La Biblioteca Central de la UNAM, en los últimos años, ha venido incrementando su infraestructura tecnológica conforme la demanda de servicios. Para satisfacer esas necesidades, se ha adquirido más equipo de cómputo para consulta de catálogos automatizados de búsqueda de libros, verificación de préstamo de libros, aulas de capacitación y préstamo de equipo para consulta de Internet, éstos últimos de manera alámbrica e inalámbrica. Con este incremento de equipo, también el equipo activo de la red se incrementa, como son los switches, firewall, servidores, etc.

A la Biblioteca Central se le asignó un segmento de red completo que, en un principio, resultó suficiente para cubrir la demanda de nodos que utilizaban la red, pero conforme se fueron incrementando, resultó insuficiente para dar cabida a los nuevos equipos y servicios. Para dar solución a este problema, en primera instancia se generó un servidor de DHCP, que cubrió durante un tiempo las necesidades de acceso a red, pero también fue sobrepasada su demanda, además de que no se tenía un control adecuado de quien se conectaba a la red, y podía acceder cualquiera que trajera una PC o una portátil.

Partiendo de lo que se logró de la segmentación de red del Departamento de Consulta, con resultados bastantes favorables, se decidió realizar la misma metodología de acceso a los servicios de red en los diferentes departamentos de la DGB.

## 1.3 Objetivo

Mejorar la administración de la red de la Biblioteca Central mediante la segmentación de redes privadas basadas en el Protocolo de Internet (IP), y tener un mejor control respecto al ancho de banda utilizado en la red, así como tener la metodología necesaria para dar respuesta al requerimiento de direcciones IP de la red.

## 1.4 Metas

Mejorar la administración de la red LAN de la DGB.

Establecer políticas de seguridad, control y mantenimiento para evitar, en lo posible, fallas de seguridad informática.

Satisfacer la demanda de los servicios de red local e Internet que se utilizan en la institución.

Liberar direcciones públicas para tenerlas disponibles para nuevos servicios o un incremento de equipos en los departamentos que lo requieran.

Mejorar el tráfico en la red y contar con las direcciones IP necesarias.

## 1.5 Estructura de la tesis

En el capítulo primero se comenta sobre la historia de la Biblioteca Central, relacionada con los sistemas informáticos y, conforme pasa el tiempo, el incremento de las demandas de servicios y equipos.

El capítulo segundo contiene la parte teórica, como son los conceptos de redes, elementos que lo integran, protocolos que se utilizan, topologías de red y el direccionamiento de IP.

El capítulo tercero se centra específicamente en las redes de tipo Ethernet, las normas que se utilizan para el cableado estructurado, los medios de transmisión disponibles y el equipo activo.

El capítulo cuarto contiene la parte del planteamiento para implementar la segmentación de la red con el sistema operativo OpenBSD en la Biblioteca Central, aquí se empieza a realizar el análisis de factibilidad de la operación. Se define cómo va a realizarse la implementación de los equipos en los diferentes niveles de la biblioteca.

El capítulo cinco muestra cómo quedó definida la red en varios segmentos, se realiza la distribución correspondiente de IP’s y las políticas de acceso que se tienen que aplicar para la puesta en marcha, así como las pruebas pertinentes. Se realiza el registro de las IP’s utilizadas y la recopilación de datos del equipo utilizado.

# CAPÍTULO 2

# TEORÍA DE REDES

## 2.1 Introducción a las redes

Uno de los grandes problemas a los que se ha tenido que enfrentar la humanidad, desde que se inventó y desarrolló la escritura, ha sido el almacenamiento y el análisis de la información que se ha generado con el tiempo. Antes de la computadora, se tenía el almacenamiento de la información en papel y en lugares destinados para ello, como son las bibliotecas personales, privadas o públicas. Con la introducción de la computadora a mitades del siglo anterior, se ha tratado de resolver este problema; sin embargo, al tener mejores capacidades de almacenamiento y transmisión, se generaron nuevos requerimientos y nueva información.

El alto costo de recursos, de espacio y almacenamiento, llevó a los fabricantes y desarrolladores a generar un nuevo concepto de trabajo; en este punto, se tuvo la idea de las redes locales LAN. Estas primeras LAN estaban basadas en Disk Servers (un primer intento), en las cuales el equipo permitía acceso aleatorio y no controlado a todos los sectores del disco, lo que causó problemas de seguridad e integridad de los datos. Posterior a esto, se utilizó el servidor de archivos, en el cual los usuarios tenían acceso a la información mediante archivos compartidos, pero en este caso ya con niveles de seguridad de acceso y modificación para cada usuario, lo que permitió la integración de la información.

Estas redes locales, basadas en el concepto de servidor de archivos, han tenido cambios conforme se han implementado nuevas tecnologías, conceptos y necesidades de todo tipo. Al inicio era difícil que el software, en este caso el operativo, soportara todos los protocolos y topologías existentes en su momento. Cuando se estandarizó esto, el problema fue la generación de métodos o procedimientos que generaran redundancia.

Con el incremento de las computadoras y su inminente introducción al ámbito educativo y comercial en los años ochenta, y personal en los noventa, se tuvo que desarrollar o mejorar las tecnologías para poder realizar las comunicaciones entre las computadoras.

La red LAN es la que ha tenido más aceptación, debido a que se tiene la facilidad de compartir los datos y recursos en un área de trabajo. Además, la posibilidad de conexión entre las redes LAN y WAN ofrece conectividad importante para las organizaciones, empresas o personas en general.

Al tener nuevas expectativas de crecimiento, con la limitante de que la LAN no satisfacía a algunos sectores de la población económicamente activa, y debido a que requerían un mejor control o manejo de la información, así como la necesidad de comunicarla e intercambiarla dentro de una área más grande, entre pequeñas y grandes empresas, así como en el ámbito educativo, se generó la idea de la MAN (Redes de área metropolitana). Este tipo de red, hoy en día, ha sido absorbido por la LAN o por la WAN, aunque lo siguen utilizando, por ejemplo, los bancos o las empresas con varias sucursales que están controladas en un área o perímetro definido por los administradores o propietarios.

Las redes de computadoras se clasifican, de acuerdo con su medida, cobertura o extensión geográfica, de la siguiente manera: LAN, MAN o WAN. Además el porqué de esta clasificación se basa en el tipo de tecnología que utilizan.

## 2.2 Elementos que integran una red

### 2.2.1 Servidor

El servidor es una computadora de alto desempeño que al formar parte de una red provee servicios de diversas características a otras computadoras de bajo desempeño que requieren utilizar el servicio. Está dentro del modelo cliente-servidor.

### 2.2.2 Estación de trabajo o computadora personal

La estación de trabajo o computadora personal es un equipo de bajo desempeño, que es utilizado para realizar procesos informáticos definidos por el usuario o la empresa, y que para poder tener interacción con otras computadoras requiere comunicarse mediante los dispositivos de la LAN o equipo activo.

### 2.2.3 Sistema operativo

El sistema operativo es el software más importante de toda computadora o servidor, dado que éste es el que realiza el reconocimiento y control del hardware interno de la computadora, el control de los periféricos y el manejo de la conexión y transferencia de la información con otro equipo. En el caso de equipos dedicados, el sistema operativo tiene más importancia y se requiere que se tenga lo más actualizado y protegido posible para evitar que los usuarios no autorizados tengan acceso a los recursos del sistema. Estos sistemas operativos pueden ser clasificados como sistemas multiusuario, multiprocesador, multitarea y en tiempo real. Los sistemas operativos proporcionan una plataforma de software en la cual

otras aplicaciones o programas funcionan. Estas aplicaciones son desarrolladas para que funcionen adecuadamente de acuerdo con el sistema operativo que se escoja o el operativo que se destina. El elegir el operativo a utilizar depende en gran medida de las aplicaciones que se requieren utilizar, o viceversa, si se le da prioridad al operativo en vez de las aplicaciones.

### 2.2.4 Tarjeta de interfaz

Las tarjetas de interfaz son los dispositivos que permiten la comunicación o enlace con la red. En la actualidad, la mayoría de las motherboards o tarjetas madre ya tienen integrado este tipo de interfaz, mas si se quiere tener uno o más interfaces extras, se tienen tarjetas externas con diferentes entradas y capacidades. Hoy en día, se utiliza el RJ45 a velocidades de 10Mbps, 100Mbps y hasta de 1Gbps, de forma teórica, cabe aclarar, ya que la velocidad no siempre será la máxima, porque depende de la calidad de hardware, software o problemas no contemplados.

### 2.2.5 Medios de transmisión

Conforme ha pasado el tiempo, se tienen diferentes tipos de conexión en la red. En un principio, las redes empezaron utilizando cable coaxial, telefónico, y posteriormente UTP (Unshielded Twisted Pair) en diferentes categorías y fibra óptica. La interfaz inalámbrica, por su naturaleza, no requiere de cableado entre el dispositivo del usuario y el punto de acceso, del punto de acceso hacia el servicio pedido depende cómo se tenga diseñado.

El cableado que se utiliza o se utilizará en las instalaciones tiene vital importancia, tanto en costos, tiempo, facilidad de instalación, distancia máxima, confiabilidad en la conexión, peso total y comunicación entre los mismos dispositivos.

Se debe tener en cuenta el tipo de topología que se esté usando, ya que esto es indicativo del tipo de cable que se requiere utilizar. En sus inicios, el cable coaxial y telefónico era el adecuado debido a su bajo costo, pero se tuvo la limitante de la respuesta de peticiones en red. Posteriormente, se utilizó el UTP, y más recientemente la fibra óptica, aunque ésta última va dedicada principalmente a equipos de alto rendimiento.

### 2.2.6 Equipo activo

Se refiere como equipo activo a los dispositivos que administran en menor o mayor medida el tráfico en la red, como son los switches, routers, o firewall vía hardware.

## 2.3 Modelos de redes de acuerdo con la cobertura

### 2.3.1 Red de área local LAN

Una Red de área local es un conjunto de elementos físicos y lógicos que se utilizan para conectar dispositivos de comunicación en un área restringida.

Por lo regular, son redes de propiedad privada o educativa que se utilizan para conectar computadoras personales o estaciones de trabajo para compartir recursos e intercambiar información en un área privada, como un edificio, un campus, un conjunto de construcciones, etc. Su tecnología de difusión es mediante par trenzado, UTP para el caso de Ethernet y STP (Shielded Twisted Pair) para el token ring. En algunos casos, se utiliza fibra óptica para los servidores.

La Red de área local, o Local Area Network, tiene una extensión de hasta un kilómetro, aunque puede extenderse un poco más. La latencia o retardo, por lo regular, es baja y con pocos errores en el caso de una red que esté correctamente instalada. La tecnología Ethernet, la token ring, y la de estrella se ubican en este tipo de red LAN. Ver imagen 2.1.

### 2.3.2 Red de área metropolitana MAN

La Red de área metropolitana MAN es una red que tiene conexión a través de diversas localidades o ciudades mediante instalaciones de carácter público o privado, variando el tipo o métodos de conexión entre los puntos de acceso, debido a las condiciones físicas y climáticas de la zona en la cual se requiere conectar para lograr lo comunicación adecuada, tales como conexión inalámbrica, fibra óptica, cable telefónico, microondas u otro tipo de tecnología.

Este tipo de redes son utilizadas dentro de empresas que ofrecen telefonía fija, telefonía celular y los proveedores de servicios de Internet. Estas empresas diseñan e implementan este tipo de redes de acuerdo con las condiciones físicas, económicas y disponibilidad de acceso con la que se tienen y cuentan en esas localidades, dentro de un perímetro establecido por zonas, como, por ejemplo, varias ciudades o un país.

Esta red dentro de la telefonía celular es muy importante, ya que es una red que está en crecimiento, así como la oferta de Internet mediante los proveedores de servicios de Internet, como es el caso en México de las empresas Telmex y su subsidiaria Telcel, BAM de Iusacell y Cablevisión, entre otras. Ver imagen 2.2.

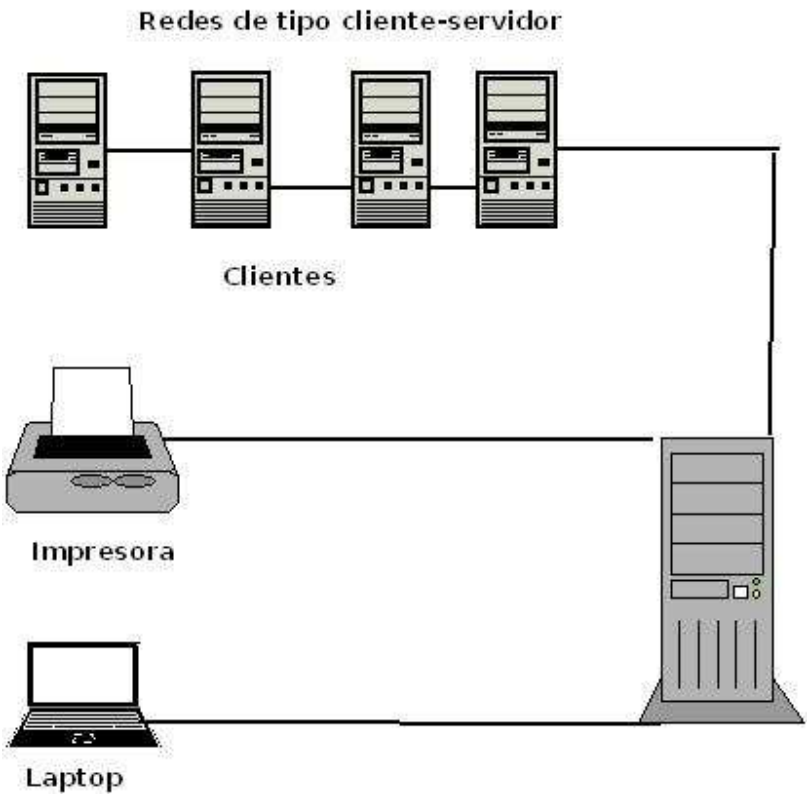



Imagen 2.1 Red de área local LAN

### 2.3.3 Red de área amplia WAN

Este tipo de redes están contenidas sobre un área geográfica extensa. Tiene un conjunto de equipos dedicados a ejecutar los programas de usuarios y están conectados para la comunicación mediante hosts. Son redes punto a punto.

Esta red tiene elementos como:

- Líneas de comunicación que mueven los bits de una máquina a otra.
- Elementos de comunicación que son máquinas especializadas que conectan dos o más líneas de transmisión llamados routers o encaminadores.

Estas redes por lo regular son proporcionadas por compañías telefónicas. La topología de estas redes WAN suele ser más irregular, debido a que tiene conexiones de diferentes tipos de velocidades.

En la imagen 2.3 se muestra la comunicación del tipo WAN.

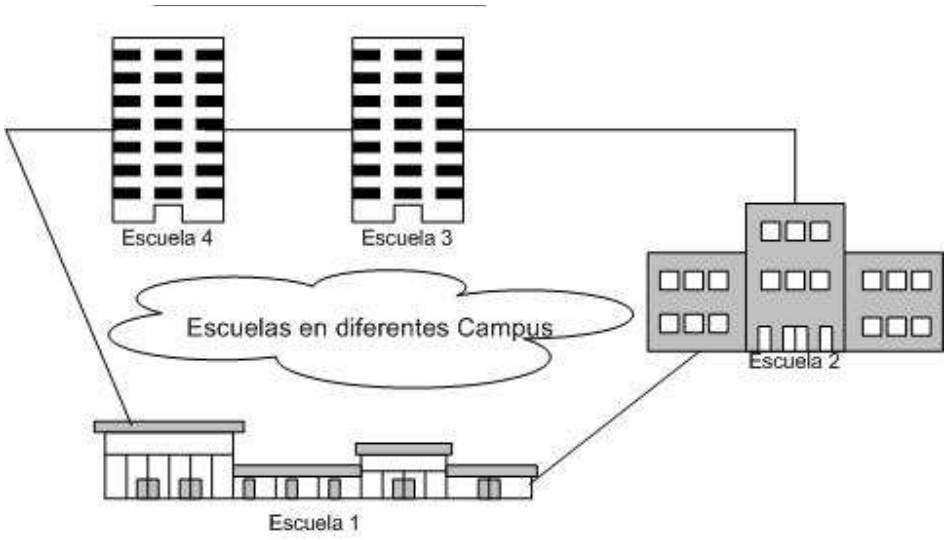



Imagen 2.2 Red de área metropolitana

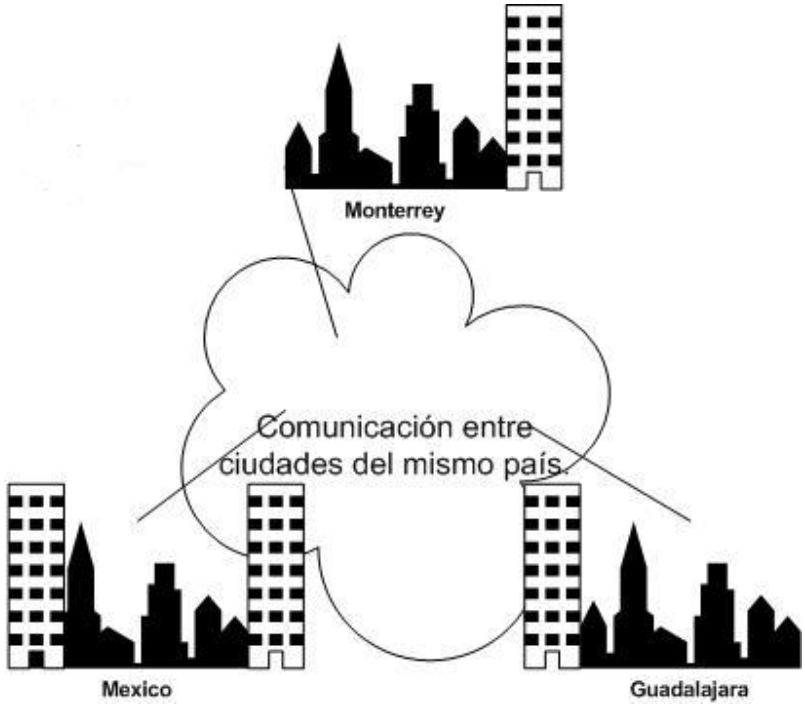



Imagen 2.3 Redes de área amplia

Los tipos de redes que se tienen son:

*Conmutadas por circuitos*: Donde la conexión se establece mediante una llamada telefónica (módem).

*Conmutadas por mensaje*: Donde el equipo es el conmutador y se encarga de aceptar el tráfico de lo que se conecta a él.

*Conmutadas por paquetes*: Donde los datos se descomponen en fragmentos pequeños y están contenidos dentro de los estándares del protocolo y recorren la red de manera independiente hasta llegar a su destino.

*Redes orientadas a conexión*: Donde se maneja la multiplexión de canales y puertos, que es conocido como canal virtual.

*Redes no orientadas a conexión o datagramas*: Donde pasan del estado libre al modo de transferencia de datos, no ofrecen confirmaciones, control de flujo ni recuperación de errores aplicables a toda la red, existiendo sólo para cada enlace particular. Un ejemplo de esta red es Internet.

*Red pública de conmutación telefónica PSTN*: es una red con conmutación de circuitos tradicional, optimizada para comunicaciones de voz en tiempo real. Cuando llama a alguien, cierra un conmutador al marcar y establece así un circuito con el receptor de la llamada. PSTN garantiza la calidad del servicio (QoS) al dedicar el circuito a la llamada hasta que se cuelga el teléfono. Independientemente de si los participantes en la llamada están hablando o en silencio, seguirán utilizando el mismo circuito hasta que la persona que llama cuelgue.

## 2.4 Topologías de red

### 2.4.1 Bus

La topología de bus es de tipo lineal, debido a que todos los dispositivos que se conectan están en el mismo canal de comunicación o backbone; es decir, todos los equipos están conectados en una sola línea. La tecnología común que trabaja con esta topología es la Ethernet.

En esta topología se tiene la ventaja de que, si algún dispositivo falla, no causa impacto en la red, debido a que el dispositivo no es responsable de pasar los datos al equipo siguiente; por consiguiente, la red no sufre caída. Ver imagen 2.4.

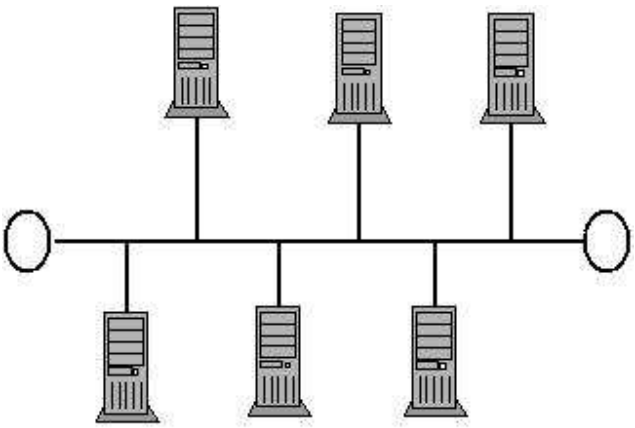


Imagen 2.4 Topología de bus

### 2.4.2 Estrella

La topología de estrella tiene una unidad central que controla la transferencia de información que mandan los nodos conectados a ella. Es una conexión punto a punto. Tiene la ventaja de centralizar los recursos mediante el nodo central, pero si el nodo o unidad central falla, toda la red se colapsa. El tamaño depende directamente de la capacidad del controlador central. Ver imagen 2.5.

Si falla un dispositivo en esta red o el cable con que está conectado, entonces el dispositivo afectado es el único que no podrá enviar o recibir datos dentro de esta red.

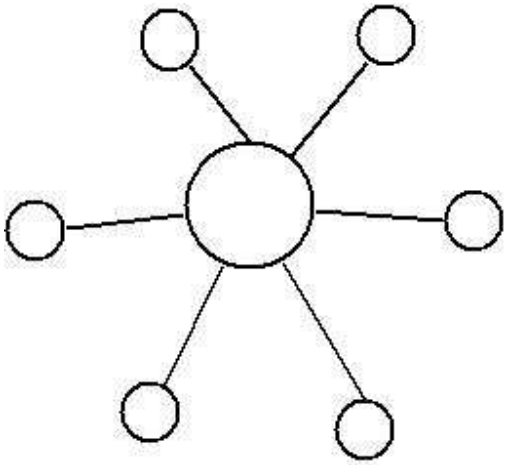


Imagen 2.5 Topología de estrella

### 2.4.3 Anillo

La característica importante de la topología de anillo es que está conectada punto a punto, formando un anillo en donde la información es enviada a través de los nodos, de nodo a nodo. Ver imagen 2.6.

La desventaja de esta topología es que, si un nodo se rompe, toda la red falla. La tecnología común de esta topología es la token ring (paso de testigo).

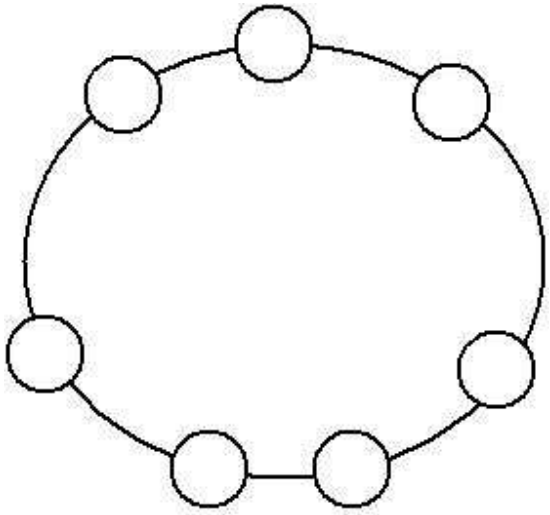


Imagen 2.6 Topología de anillo

### 2.4.4 Malla

La topología de malla ofrece redundancia y fiabilidad superiores a las demás topologías, debido a que cada equipo de la red está conectado a todos los demás de manera independiente mediante cables o conexiones separadas.

Este tipo de topología, por su naturaleza, es muy costosa de cubrir, debido a que se multiplica su costo por la cantidad de dispositivos que se desea conectar. Ver imagen 2.7.

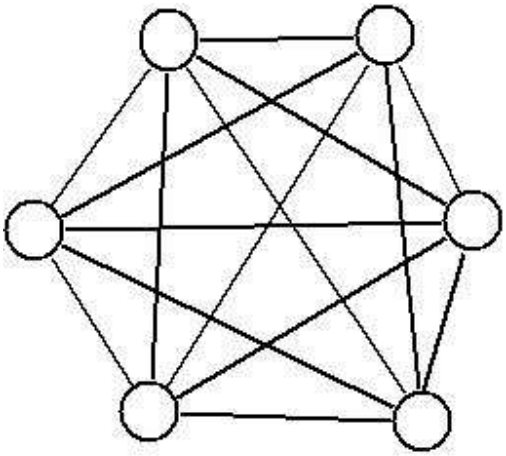


Imagen 2.7 Topología de malla

### 2.4.5 Jerárquica

La topología jerárquica fue de las primeras topologías diseñadas para las redes LAN, y es de las más utilizadas en las redes WAN. Trabaja basada en la distribución jerárquica de los dispositivos en un bus donde la información tiene que llegar siempre a la cabecera de jerarquía. Ver imagen 2.8.

### 2.4.6 Híbridas

Las topologías híbridas son redes que trabajan dos o más tipos de topología, los cuales son utilizados debido a características especiales, condiciones geográficas del lugar o por políticas de acceso.

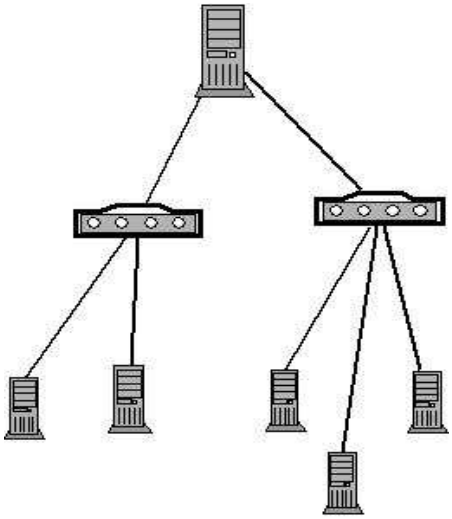


Imagen 2.8 Topología jerárquica

## 2.5 Modelo OSI y modelo TCP/IP

### 2.5.1 Modelo OSI

El modelo de interconexión de sistemas abiertos (OSI), desarrollado por el International Standard Organization (ISO), es un conjunto de especificaciones que normalizan la arquitectura de red para la conexión de dispositivos diferentes, permitiendo que los usuarios se puedan comunicar mediante estos dispositivos sin tener que preocuparse de cómo lo hacen. Este modelo permite localizar problemas de una manera modular, proporcionando un marco de referencia que describe el supuesto funcionamiento de los componentes. En la imagen 2.9 se muestra la comunicación entre dos puntos utilizando el modelo OSI.

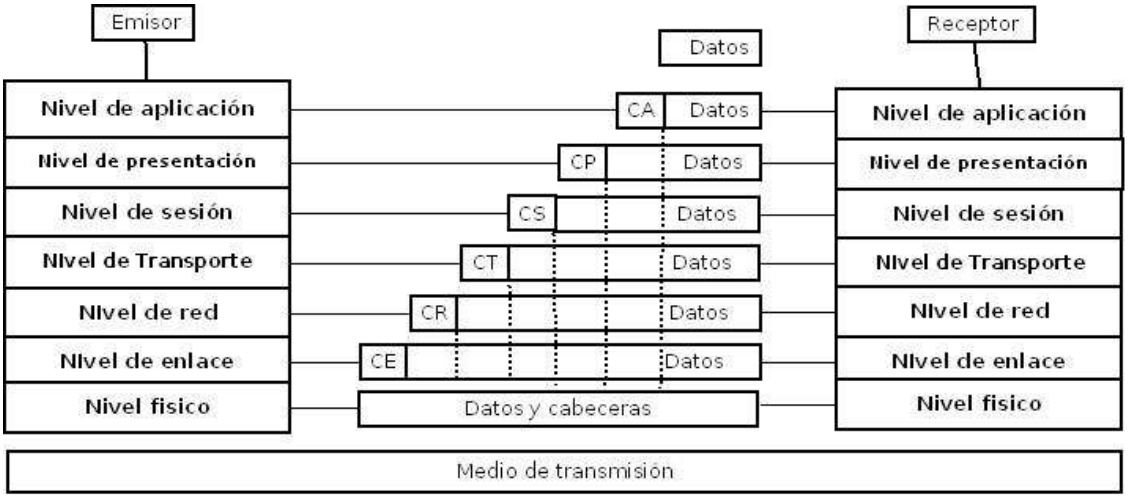



Imagen 2.9 Comunicación del modelo OSI

El modelo OSI se forma por siete capas y el intercambio de información se da entre capas del mismo nivel. La comunicación entre capas de un mismo sistema se da entre la capa inmediata superior y la capa inmediata inferior.

Cada capa proporciona algún servicio o acción que prepara los datos para entregarlos a través de la red a otro equipo. Las capas inferiores (1 y 2) definen el medio físico de la red y las tareas relacionadas, como la colocación de los bits de datos sobre las placas de red (NIC, Network Interface Cards) y el cable. Las capas superiores definen la forma en que las aplicaciones acceden a los servicios de comunicación. Mientras más alta es la capa, más compleja es su tarea.

Las capas están separadas entre sí por fronteras, llamadas interfaces. Todas las demandas se pasan desde una capa, a través de esta interfaz, hacia la siguiente.

Cada capa se basa en los estándares y actividades del nivel inferior. Ver imagen 2.10.


Imagen 2.10 Capas del modelo OSI

### 2.5.1.1 Capa física

La capa física es la que se comunica con el medio de comunicación de manera directa a nivel de bits. Se definen parámetros como:

- El voltaje a utilizar 1 o 0
- La duración del voltaje para el bit transmitido
- La asignación del nivel de voltaje 1 a utilizar
- Sincronización
- Conectores físicos
- Distancia en la conexión

### 2.5.1.2 Capa de enlace

La capa de enlace es la encargada de proporcionar confiabilidad en la transmisión de la información que realiza la capa física mediante la detección y corrección de errores.

Se encarga de proporcionar un mecanismo de direcciones que permiten entregar la información en los nodos correctos, además de traducir los mensajes de las capas superiores en bits para que puedan ser transmitidos en la capa física; esto lo hace mediante la utilización de frames o tramas que dividen en paquetes los datos a enviar; las secciones de una trama de datos se denominan campos.

A estos campos se les agrega información de:

- Dirección de origen y destino
- Delimitadores
- Tamaño del paquete

Además se definen especificaciones como:

- Direccionamiento físico
- Topología de red
- Notificación de errores
- Control de flujo
- Secuencia de tramas

La capa de enlace de datos se divide en dos subcapas. La subcapa LLC y la Subcapa MAC. Ver imagen 2.11.

La LLC, o Logical Link Control, es la capa superior, la cual permite la conexión entre diferentes tipos de redes, controla las transmisiones y recepción de las tramas y detecta los errores producidos por la capa física.

La MAC, o Media Access Control, es la subcapa inferior, y se encuentra más relacionada con el medio físico, controla el acceso al medio para la transmisión y realiza la fragmentación de los datos en tramas.

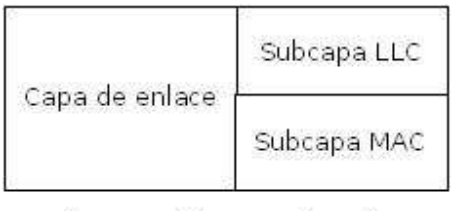



Imagen 2.11 Subcapas de la capa de enlace

### 2.5.1.3 Capa de red

La capa de red es la que establece, mantiene y termina la conexión con la red. Determina la ruta a seguir para el envío de la información entre dos nodos sobre la red. Realiza evaluaciones para la mejor transmisión en función de diversos parámetros, como el tráfico de la red o las nulas respuestas.

Esta capa de red opera de manera independiente del medio físico, que es competencia de la capa física.

#### 2.5.1.4 Capa de transporte

La capa de transporte es la encargada de dar confiabilidad al enlace de red, proveyendo la corrección de errores, como las duplicidades, orden, coherencia, pérdida y retrasos, para garantizar el correcto control de flujo entre los dos nodos que se quieren comunicar.

Esta capa acepta los datos de la capa de sesión y los divide en unidades más pequeñas, después los pasa a la capa de red y se asegura de que estas unidades lleguen correctamente al otro extremo.

#### 2.5.1.5 Capa de sesión

La capa de sesión es la que permite la comunicación entre dos nodos, establece su sincronización y la interacción entre éstos, y empieza, administra y termina las conexiones a nivel lógico.

Establece el tipo de comunicación que deben tener los nodos para interactuar, dependiendo de la red. Éstos son: simplex, half duplex o full duplex.

#### 2.5.1.6 Capa de presentación

La capa de presentación es la que realiza la presentación de los datos adquiridos, enviados por un nodo de una manera en que las aplicaciones que tiene el nodo puedan entender. Esta capa provee los servicios como el formato de los datos y la asignación del tipo de aplicación requerida.

Esta presentación o transformación de los datos es la que permite que diferentes aplicaciones se puedan comunicar entre sí, aunque utilicen métodos diferentes para representar los mismos datos.

#### 2.5.1.7 Capa de aplicación

La capa de aplicación es la que provee el servicio que se requiere, de manera directa, al usuario, siendo ésta la más cercana a él. Es la que provee los servicios a los programas que se muestran en la interfaz del usuario, así como las herramientas que el usuario utiliza para acceder a la red.

### 2.5.2 El Modelo TCP/IP

Los protocolos de comunicación son reglas y procedimientos para la comunicación, los cuales crean los estándares de conexión de las redes

desarrolladas. Estos protocolos pueden trabajar en jerarquía o en conjunto con otros protocolos.

En general, los protocolos funcionan de la manera siguiente:

Los protocolos en el equipo origen se dividen en secciones más pequeñas (paquetes), se añade la información sobre la dirección de manera que el equipo destino determine si los datos enviados son para él, y prepara los datos para transmitirlos a través de la NIC y enviarlos a través de la red.

Los protocolos en el equipo destino constan de la misma serie de pasos, pero inversamente; es decir, toma los paquetes de datos de la red y a través de la NIC los recibe, extrae los paquetes de datos de la información, elimina la información añadida por el equipo origen, y copia los datos de paquetes para reorganizarlos y enviarlos a la aplicación que lo solicitó.

El TCP/IP (Transmission Control Protocol / Internet Protocol) es un conjunto de protocolos que permiten la comunicación en diferentes ambientes de redes o un entorno heterogéneo, que está formado por elementos diferentes. Esto debido a que soporta ruteo o red encaminable y permite acceder a Internet y sus recursos, permitiendo la comunicación a través de segmentos. Es el protocolo estándar para la comunicación sobre el Internet, y su principal ventaja es la interoperabilidad.

La mayoría de las redes permiten a TCP/IP como protocolo, y se utiliza como un protocolo de interconexión de redes. Este protocolo tiene varias ventajas, como la de ser un estándar en la industria, contener un conjunto de utilidades para la conexión de sistemas operativos diferentes y utilizar una arquitectura escalable de cliente-servidor.

Este conjunto de protocolos utiliza cuatro capas en su modelo de comunicación para transmitir los datos de un punto a otro. Estas capas son: aplicación, transporte, Internet y la interfaz de red. Ver imagen 2.12.

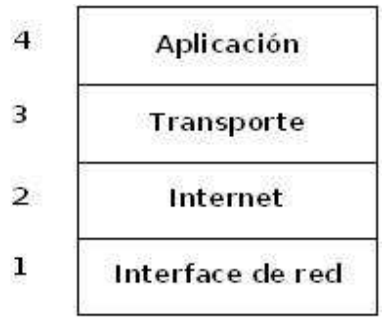



Imagen 2.12 Capas del modelo TCP/IP

#### 2.5.2.1 Capa de interfaz de red

La capa de interfaz de red es la que introduce los datos en el medio de la red. Contiene los dispositivos físicos de la red, como cables y adaptadores de red. Tiene los protocolos asociados de Ethernet, ATM y token ring, los cuales definen cómo son transmitidos los datos a la red.

#### 2.5.2.2 Capa de Internet

La capa de Internet es la que se encarga de direccionar, empaquetar y rutear los datos para ser transmitidos. Esta capa tiene cuatro protocolos asociados:

- Internet Protocol (IP). Realiza la transferencia o direccionamiento de los datos para ser enviados a su destino mediante el uso de direcciones, las cuales permiten el ruteamiento.

- Address Resolution Protocol (ARP). Este protocolo identifica la dirección MAC que corresponde a la dirección de hardware NIC en la computadora destino. Realiza el mapeo de dirección IP a dirección física. Si la ARP no contiene la dirección en su propio caché, envía una petición por toda la red, solicitando la dirección. Todos los hosts de la red procesan la petición y, si contienen un valor para esa dirección, lo devuelven al solicitante.

- Internet Control Message Protocol (ICMP). Es utilizado para enviar y recibir informes de estado sobre la información que se está trasmitiendo. Estos paquetes suelen determinar cómo va la conectividad entre dos hosts. Los routers suelen utilizar el ICMP para controlar el flujo o velocidad de datos entre ellos.

- Internet Group Management Protocol (IGMP). Administra el multicasting.

- Reverse Address Resolution Protocol (RARP). Este protocolo proporciona una dirección IP a una petición con dirección de hardware. Cuando un servidor RARP recibe la petición de un número IP desde un nodo de red, responde comprobando su tabla de encaminamiento para el número de máquina del nodo que realiza la petición y le devuelve la dirección IP.

#### 2.5.2.3 Capa de transporte

La capa de transporte es la encargada de transmitir de manera confiable datos de un nodo a otro. Se encarga de pasar los datos de la capa de aplicación hacia la

capa de Internet. Es un protocolo orientado a la conexión y establece una conexión o sesión entre dos máquinas antes de transferir la información. Especifica un identificador único de aplicación para el cual los datos son enviados y tiene dos protocolos que controlan el método por el cual serán enviados: el protocolo TCP y el UDP.

- Transmission Control Protocol (TCP). Es el responsable de la transmisión confiable de los datos. Crea una conexión entre los dos nodos mediante el uso de un número especial, llamado puerto, para averiguar a qué aplicación hay que entregarle el paquete. Realiza la detección de errores desde un nodo a otro, así como la recuperación del flujo de datos. También segmenta y ensambla los datos del usuario y protocolos de capas superiores.

  Para establecer una conexión fiable, TCP establece el número de puerto y los números de secuencia de inicio desde ambos lados de la transmisión. El acuerdo consta de tres pasos:

  a) El solicitante envía al destino un paquete, especificando el número de puerto que él planea utilizar y el número de secuencia inicial (ISN).

  b) El servidor destino responde con su ISN, que consiste en el ISN del solicitante más uno.

  c) El solicitante responde a la respuesta del servidor con el ISN del servidor más uno.

- User Datagram Protocol (UDP). Trabaja bajo el modelo “sin conexión”, donde no existe un control de flujo, por lo que es capaz de proveer un rápido envió de paquetes, pero no garantiza la entrega de los mismos. Los mensajes pueden perderse, duplicarse o llegar desordenados. En general, UDP se utiliza para enviar pequeñas cantidades de datos que no necesitan una entrega garantizada, y aunque UDP utiliza puertos, son distintos de los puertos TCP, de tal manera que se pueden utilizar los mismos números sin interferirse.

### Puertos y sockets

Los números de puertos del protocolo se utilizan para localizar una aplicación o proceso en particular en cada nodo en el nivel de aplicación. El puerto identifica la dirección de un host en la red, el número de puerto identifica la aplicación a nivel de transporte, por lo que proporciona una conexión completa de una aplicación de un host a una aplicación de otro host. Las aplicaciones y servicios pueden configurar hasta 65536 puertos. Las aplicaciones y servicios TCP/IP utilizan los primeros 1023 puertos. Cualquier aplicación del cliente puede asignar números de puerto dinámicamente cuando sea necesario.

Un puerto y una dirección de nodo o IP forman un socket. Los servicios y aplicaciones utilizan sockets para establecer conexiones con otro hosts. Si las aplicaciones necesitan garantizar la entrega de datos, el socket elige el servicio orientado a conexión (TCP); si no se requiere, se escoge la conexión por UDP.

#### 2.5.2.4 Capa de aplicación

La capa de aplicación es la que realiza la conexión entre las aplicaciones y utilerías de red. Los protocolos en esta capa son usados para intercambiar información del usuario; entre éstos, figuran los siguientes:

- Hypertext Transfer Protocol (HTTP). Se utiliza para que los servidores envíen páginas web a los clientes, mediante navegadores por el puerto 80.

- File Transfer Protocol (FTP). Transfiere información mediante archivos entre servidores y clientes; utiliza el puerto 21 para el control de los mensajes y envía los datos usando el puerto 20.

- Simple Mail Transfer Protocol (SMTP). Es para el envío del correo electrónico; utiliza el puerto 25. Algunos clientes o servidores utilizan otros puertos, pero éste es el común.

- Post Office Protocol Version 3 (POP3). Permite al software cliente de correo electrónico recibir el correo electrónico de un servidor de correo, utilizando el puerto 110.

- Simple Net Management Protocol (SNMP). Permite a las aplicaciones de administración de red controlar remotamente otros dispositivos de red, mediante el puerto 161.

- Telnet. Permite al usuario iniciar una sesión remota y ejecutar comandos basados en texto, empleando el puerto 23.

## 2.6 El direccionamiento IP

### 2.6.1 Dirección IP

La utilización de las direcciones IP permite reconocer una interfaz de red de un dispositivo dentro de una red que esté utilizando el protocolo IP, y permite su ruteo.

Para la utilización de IPv4 se especifica que sus direcciones están formadas por 32 bits, que a su vez se agrupan en cuatro grupos de 8 bits u octetos, los cuales son separados por un punto y luego son interpretados en forma decimal para el usuario. Un ejemplo de esto es el siguiente:

132.248.67.22=10000100.11111000.01000011.00010110

Cada octeto toma valores desde 0 hasta 255 en notación decimal. Serían 256 valores y va del 0 (00000000), hasta el 255 (11111111).

A ningún equipo se le debe asignar su identificador de hosts a ceros o a unos, porque el cero es utilizado para la identificación en red y los unos se utilizan para el broadcast, que es la comunicación con todos los hosts de la red local.

La ICANN (Internet Corporation for Assigned Names and Numbers - Corporación de Internet para la asignación de nombres y números) es la responsable de la coordinación global del sistema de direcciones IP.

### 2.6.2 Máscara de red

La máscara de red es un conjunto de 32 bits agrupados en 4 octetos separados por puntos, y se utiliza para conocer los identificadores de red y de host de una dirección IP. De la máscara, las posiciones de los bits en uno se consideran parte del espacio reservado para la dirección de red, mientras que los bits en cero se consideran parte del espacio apartado para el número de máquina.

Se muestran los siguientes ejemplos y notaciones:

11111111.11111111.11111111.00000000=255.255.255.0=/24
11111111.11111111.00000000.00000000=255.255.0.0=/16
11111111.00000000.00000000.00000000=255.0.0.0=/8

### 2.6.3 Clases

Las direcciones IP están separadas en cinco grupos, como se muestran en la tabla 2.1

| Clase | Rango de direcciones IP | Redes | Hosts por red | Máscara de subred |
|---|---|---|---|---|
| A | 1.0.0.0 – 126.255.255.255 | 126 | 16777214 | 255.0.0.0 |
| B | 128.0.0.0 – 191.255.255.255 | 16382 | 65534 | 255.255.0.0 |
| C | 192.0.0.0 – 223.255.255.255 | 2097150 | 254 | 255.255.255.0 |
| D | 224.0.0.0 – 239.255.255.255 | Reservadas para multicast | | |
| E | 240.0.0.0 – 255.255.255.255 | Reservadas para uso futuro | | |

Tabla 2.1 Clases de IP

El rango de direcciones faltantes que va de la IP 127.0.0.0 al 127.255.255.255 está reservado para pruebas internas del mismo equipo. Se denomina loopback.

Se identifican cinco tipos de clase, su rango de direcciones, la cantidad de redes y hosts por red, así como la máscara de red que utilizan.

### 2.6.4 Direcciones IP públicas y privadas

En términos generales, una IP pública puede conectarse directamente a la red.

Las redes privadas, por el contrario, no se conectan directamente a la red; éstas requieren de un equipo, servidor proxy o un router para poder salir a red. Estas direcciones privadas se emplean cuando no se tienen suficientes direcciones IP dentro de una organización, o para ocultar estos equipos de otras redes; también se usan cuando no se requieren muchas IP’s públicas en el caso de las empresas.

Estas direcciones privadas tienen un rango de direcciones IP definido. De acuerdo con la clase a la que pertenecen, éstas son las siguientes:

Clase A 10.0.0.0 - 10.255.255.255
Clase B 172.16.0.0 - 172.31.255.255
Clase C 192.168.0.0 - 192.168.255.255

# CAPÍTULO 3

# REDES ETHERNET

## 3.1 Introducción

Las redes LAN Ethernet han tenido un gran auge debido al bajo costo. Los medios de comunicación dentro de las redes Ethernet, conforme pasa el tiempo, van mejorando, o en su defecto, sustituyéndose por otras tecnologías mejor adaptadas para la demanda de información.

El hardware en donde se realiza este tipo de control de flujo de información, o que se encarga de mantener la comunicación constante de información entre los nodos de la red, se reconoce como equipo activo. Partes del equipo activo son los hubs, switches, routers, firewall, medios de control de flujo vía hardware, como antispam, etc.

Para que la red esté completamente activa, también se requiere el medio de comunicación o el tipo de conexión, que sería alámbrica o inalámbrica; para nuestro caso, estamos centrándonos en la red Ethernet de tipo alámbrica. En el caso de que se planee o decida tener un medio de comunicación o conexión para el equipo activo bastante bien formado y planeado, ya estaríamos hablando de un cableado estructurado.

## 3.2 Estándares de redes

En el capítulo anterior, se explicó cómo funciona el modelo TCP/IP y su relación con el modelo OSI. Estos modelos TCP/IP y OSI en realidad son un conjunto de protocolos, que definen determinados procedimientos en la medida de las necesidades que la red tenga, en este caso la red Ethernet. Debido a la implementación de las redes, se tuvo necesidad de crear estos procedimientos y normarlos, mejorarlos, incrementarlos o diseñar nuevos.

### 3.2.1 Estándar OSI

Para el caso referido del modelo OSI, el organismo encargado de definir las reglas para la comunicación de este modelo es el IEEE (The Institute of Electrical and Electronics Engineers Inc.). Este organismo tiene normas en diferentes ámbitos de la ingeniería eléctrica y electrónica, que se toman en buena parte para el diseño o implementación de los servicios que se requieran.

Un ejemplo de esto es el IEE802, sobre el que se definen estándares para las redes de computadoras, relacionadas concretamente para redes LAN y MAN, y entre las cuales de manera más específica se puede hacer mención de redes Ethernet (IEE 802.3) o Wi-Fi (IEE 802.11). De manera general, se enlistan los estándares que están dentro de la IEE802:

IEEE 802.1 – Normalización de interfaz
IEEE 802.2 – Control de enlace lógico
IEEE 802.3 – CSMA/CD (Ethernet)
IEEE 802.4 – Token bus
IEEE 802.5 – Token ring
IEEE 802.6 – MAN (ciudad) (fibra óptica)
IEEE 802.7 – Banda ancha
IEEE 802.8 – FDDI (fibra óptica)
IEEE 802.9 – Voz y datos en LAN
IEEE 802.10 – Seguridad
IEEE 802.11 – Redes inalámbricas WLAN
IEEE 802.12 – Prioridad por demanda
IEEE 802.14 – Módem de cable
IEEE 802.15 – WPAN (Bluetooth)
IEEE 802.16 - Redes de acceso metropolitanas sin hilos de banda ancha (WIMAX)
IEEE 802.17 – Anillo de paquete elástico
IEEE 802.18 – Grupo de Asesoría Técnica sobre Normativas de Radio
IEEE 802.19 – Grupo de Asesoría Técnica sobre Coexistencia
IEEE 802.20 – Mobile Broadband Wireless Access
IEEE 802.21 – Media Independent Handoff
IEEE 802.22 – Wireless Regional Area Network

## 3.3 Ampliación de la red

Conforme se diseña una red, se van generando nuevas necesidades, debido al incremento de recursos humanos, servicios de información, almacenamiento, etc. Para satisfacer estas necesidades crecientes de la organización, se requiere ampliar el tamaño o mejorar el rendimiento de la red instalada dentro del entorno permisible, aunque llegará el momento en que la red simplemente no puede llegar a expandirse más, debido a las mismas limitaciones de las topologías y arquitectura de red.

### 3.3.1 Switch

El switch es un dispositivo de enlace de redes de computadoras que opera en capa 2, 3 o 4 del modelo OSI. La principal función de éste es realizar la intercomunicación de dos o más segmentos de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino.

Éstos se utilizan cuando se desea conectar múltiples redes o como ampliación de la misma, y mejoran el rendimiento y seguridad de la Red de área local.

Los switches se pueden conectar unos con otros, pero de forma que exista un único camino entre dos puntos de red. En caso de no seguir la regla, se forma un loop que produce la transmisión infinita de las tramas de un segmento a otro. De manera general, estos dispositivos utilizan el algoritmo de spanning tree para evitar loops, haciendo la transmisión de datos segura respecto a la conectividad.

Un punto crítico de los switches son los loops, que consisten en habilitar dos caminos diferentes para llegar a un solo destino a través de un conjunto de switches. Estos loops se realizan porque el switch detecta que el dispositivo es accesible a través de dos puertos y que emiten la trama por ambos. Al llegar esta trama de datos al switch siguiente, se vuelve a enviar por los puertos que permiten alcanzar el equipo. Este proceso provoca que cada trama se multiplique de manera exponencial conforme a la cantidad de switches involucrados, llegando a producir el colapso de la red o caída de comunicaciones.

Los switches se pueden clasificar por método de direccionamiento respecto a las tramas utilizadas, como el store and forward, cut through y fragment tree, o por la forma de segmentar las subredes en capa 2, 3 y 4, principalmente.

#### 3.3.1.1 Store and forward

Los switches store and forward guardan una trama en su buffer de almacenamiento antes de enviarlo de salida. El switch calcula el CRC (Cyclic Redundancy Check) y su tamaño de la trama mientras se encuentra en el buffer. Si la trama tiene un problema en su contenido, entonces se descarta; si pasa la revisión, es enviada al puerto de salida.

Estos switches tienen como ventaja que aseguran operaciones sin error y se aumenta la confianza en la red. La desventaja es que cada trama revisada incrementa el tiempo de respuesta de la información solicitada, debido al procesamiento y revisión de las mismas tramas en el switch, resultando en tiempos de respuestas proporcional al tamaño de las tramas.

### 3.3.1.2 Cut through

Los switches cut through fueron diseñados para resolver el problema que tienen los de tipo store and forward. Muestra un retardo mucho menor de la trama, en el cual se leen sólo los 6 primeros bytes de datos que contiene la dirección de destino MAC, y la encaminan de manera inmediata.

Este modelo o tipo de switch no detecta las tramas corruptas que son causadas por las colisiones, ni los errores de CRC. Si se incrementa el número de colisiones en la red, se incrementará el ancho de banda consumido.

### 3.3.1.3 Fragment tree

El switch fragment tree es del mismo tipo cut through, pero la diferencia se encuentra en que se leen los primeros 64 bytes de datos de la trama, que es el mínimo de tamaño de la trama (el máximo es 1518bytes), evitando así menos colisiones en la red.

### 3.3.1.4 Adaptative cut through

Los tipos de switch adaptative cut through soportan los métodos store and forward y cut through. Se puede activar cualquier modo para realizar la administración de la red o de manera automática el switch lo puede realizar, considerando el número de tramas con error que pasan por los puertos activos.

En la imagen 3.1 se da una muestra de switch Extreme Networks que trabaja a capa 3 del modelo OSI con puertos configurables a 10Base-T y a 100Base-Tx. Soporta protocolo spanning tree y manejo de VLAN’s.

Imagen 3.1 Switch

### 3.3.1.5 Switch de capa 2

Los switches de capa 2 son los dispositivos que funcionan como puentes multipuertos, los cuales son los más usados en las redes Ethernet. La función principal consiste en dividir una LAN en múltiples dominios de colisión. Basan su decisión de envío en la dirección MAC destino que contiene cada trama. Estos switches de nivel 2 del modelo OSI realizan transmisiones simultáneas sin interferir en otras subredes.

La desventaja es que no filtran difusiones o broadcast, multicast ni tramas cuyo destino aún no haya sido incluido en la tabla de direccionamiento.

### 3.3.1.6 Switch de capa 3

Los switches de capa 3 cubren las funciones de los de capa 2; además, incorporan algunas funciones de enrutamiento, como la del mejor camino, validación de la integridad del cableado vía checksum y protocolos de ruteo tradicionales, como el RIP y el OSPF. Soportan la implementación de redes virtuales (VLAN's) y, dependiendo de las marcas y modelos, la comunicación entre VLAN's sin necesidad de ruteo externo.

Este tipo de switch es utilizado en las redes LAN con un número grande de nodos, porque se permite la unión de segmentos de diferentes dominios de difusión o broadcast. Si se utilizaran switches de capa 2 en estas áreas o redes grandes, el resultado sería tener una pérdida en el rendimiento de la red, debido a la cantidad excesiva de broadcast.

Los switches de capa 3 pueden operar de las siguientes formas:

*Paquete por paquete (PPL3):* Este tipo de switch es un caso especial de store and forward: almacena y examina el paquete, calcula el CRC y decodifica la cabecera de la capa de red, para definir su ruta a través del protocolo de enrutamiento adoptado.

*Cut Through Layer 3 (CTL3):* Examina los primeros campos, determina la dirección de destino a partir de las cabeceras de capa 2 y 3, y a partir de ese punto establece una conexión punto a punto (nivel 2) para conseguir una alta transferencia de paquetes.

Para la identificación correcta del flujo de los datos, cada fabricante tiene un "standard" propio.

Un ejemplo de switch de capa 3 es el switch Alpine 3808, como el que se muestra en la imagen 3.2. Este switch es capa 3, con interfaces 10/100/1000 de

transmisión, ubicado en el cuarto de control principal de la Dirección General de Bibliotecas, escalable y conectividad con fibra óptica.


Imagen 3.2 Switch Alpine

### 3.3.1.7 Switch de capa 4

El switch de capa 4 maneja la información de los encabezados de los paquetes, en los que se incluyen capas 2 y 3, como el TTL y checksum de la 3. Se maneja información relevante, como el tipo de protocolo capa 4 a usar, como el UDP o TCP y el número de puerto. Son conocidos como switches sin capa. Son switches capa 3 que procesan el encabezado de la capa 4.

La información del encabezado de capa 4 permite clasificar de acuerdo con secuencias de paquetes manejados por aplicación; éstos se denominan “flujos”. Dependiendo de cómo se diseña el switch, éste puede dar prioridad a determinados servicios o ancho de banda por “flujos”. Algunos de estos diseños son:

*Arquitectura basada en crossbard:* Proveen prioridad por flujo.

*Switches con memoria compartida y cola de salida:* Manejan múltiples niveles de prioridad. El número de flujos no debe exceder el número de colas.

*Switches con colas por flujos:* Garantizan ancho de banda y manejan bien el tráfico. Hace relación de un flujo por una cola de salida, relación uno a uno.

### 3.3.2 Router

El router es un dispositivo electrónico con la capacidad para distribuir cada paquete de información que recibe, y que además decide la manera más conveniente de enviarlo al destino, operando en capa 3. Es la pieza fundamental de cualquier red electrónica de comunicaciones.

Se compone de una interfaz de red, la cual conecta a una o más redes que usan protocolos de capa 3, maneja tablas de ruteo y un determinado algoritmo de ruteo como RIP u OSPF.

El funcionamiento en forma general de un router es el siguiente:

- Del host origen, los paquetes se envían al proveedor de servicios.
- El proveedor de servicios deriva los paquetes a un router.
- El router analiza el envío y consulta su tabla de enrutamiento. Revisando la dirección IP origen.
- Basándose sobre ciertos factores, determina la ruta ideal. Éstos son: cuenta de saltos, condiciones de tráfico, velocidad de la línea, costo de transmisión, etc. El protocolo de ruteo es el que determinará qué factores tomará en cuenta.
- Si el router decide utilizar cuenta de saltos, toma el camino más corto. Pero si encuentra tráfico excesivo, revisa otra ruta alternativa.
- La información viaja de router en router, y cada paquete viaja por una ruta definida entre routers.
- El último router de la cadena reúne los paquetes que conforman el envío y lo encamina al host de destino.

Tipos de router:

A) Conectividad small office, home office (SOHO)

Éstos se utilizan con frecuencia en los hogares para conectar un servicio de banda ancha sobre cable o DSL. La imagen 3.3 es una muestra de este tipo de router.


Imagen 3.3 Router tipo SOHO

B) Enrutadores de empresa

Los más completos suelen estar en ISP's, instituciones académicas y de investigación. En la imagen 3.4, se puede ver un router del tipo empresarial.

Se separan en los siguientes grupos:

- Acceso. Se encuentran en sitios de clientes, como sucursales que no necesitan enrutamiento jerárquico. Son utilizados por el bajo costo.

- Distribución. Estos routers agregan tráfico desde enrutadores de acceso múltiple, ya sea del mismo lugar o de la obtención de los flujos de datos procedentes de diferentes sitios. Aplican calidad en el servicio a través de la WAN, por lo que deben de tener memoria considerablemente grande, varias interfaces WAN y buenos algoritmos de ruteo.

- Núcleo. El core router es un dispositivo diseñado para operar en el backbone principal del campus o de múltiples edificios. Son optimizados para el ancho de banda alto.


Imagen 3.4 Router empresarial

## 3.4 Firewall

El firewall es un sistema diseñado para prevenir acceso no autorizado hacia o desde una red privada. Usualmente protege la red privada de una empresa de las redes públicas o compartidas a las que se conecta. Un firewall puede ser tan simple como un ruteador que filtra paquetes, o tan complejo como varios ruteadores o varias computadoras que combinan el filtrado de paquetes con servicios proxy a nivel aplicación. Pueden ser implementados en hardware, en software, o bien una combinación de ambos.

Generalmente, los firewalls son utilizados para evitar el acceso no autorizado a usuarios del exterior hacia el interior de la empresa; es decir, del Internet hacia la Intranet de la empresa. De acuerdo con la forma en que se definan las políticas de acceso, las peticiones que entran o salen de la Intranet-Internet pasan a través del firewall, el cual examina cada mensaje y bloquea aquellos que no cumplen las políticas de seguridad especificadas. Las políticas de seguridad son el conjunto de reglas de seguridad, convenciones y procedimientos establecidos para realizar las comunicaciones dentro y fuera de una red determinada.

Un firewall es considerado la primera línea de defensa para proteger la información privada.

En la imagen 3.5 se muestran 2 equipos firewall ubicados en el cuarto de comunicación de la Dirección General de Bibliotecas. Un equipo Fortigate 800 y un Barracuda Spam Firewall 800, montados en rack.


Imagen 3.5 Firewall

## 3.4.1 Técnicas de implementación de un firewall

### 3.4.1.1 Filtros a nivel paquete (Packet Filters)

Los filtros a nivel paquete son la primera generación de firewalls, la cual analiza el tráfico de la red. Cada paquete que entra o sale de la red es analizado y lo acepta o rechaza, basándose en reglas definidas por el usuario. El filtrado de paquetes es efectivo y transparente para los usuarios de la red. Tiene la desventaja de ser susceptible a IP spoofing.

El firewall tiene los siguientes pasos, de acuerdo con la manera como se configure: Al encontrar una regla para aplicar al paquete y ésta le permite el paso, el paquete es aceptado. Si la regla niega el paso del paquete, éste es rechazado. Si no se tienen reglas para aplicar al paquete, entonces es rechazado.

### 3.4.1.2 Firewall a nivel circuito (Circuit Level Firewalls)

La segunda generación de firewalls son los llamados a nivel circuito. Revisan que los paquetes sean de una solicitud de conexión o de una conexión entre dos computadoras, y aplican mecanismos de seguridad cuando una conexión TCP o UDP es establecida. Una vez que la conexión se establece, los paquetes transmitidos ya no son revisados por las medidas de seguridad tomadas anteriormente.

El firewall mantiene temporalmente una tabla de conexiones válidas y permite que los paquetes de la red pasen a través de ella si corresponden a algún registro de la tabla. Una vez terminada la conexión, la tabla se borra y la transmisión de información entre las dos computadoras se cierra.

### 3.4.1.3 Firewall a nivel aplicación (Application Layer Firewalls)

La tercera generación de firewalls son a nivel aplicación. Éstos examinan la información de todos los paquetes de la red, y mantienen el estado de la conexión y la secuencia de la información. En este tipo de tecnología, también se puede validar claves de acceso y algunos tipos de solicitudes de servicios.

La mayoría de estos tipos de firewalls requieren software especializado y servicios proxy. Un servicio proxy es un programa que aplica mecanismos de seguridad a ciertas aplicaciones, tales como FTP o HTTP. Un servicio proxy puede incrementar el control al acceso, realizar chequeos detallados a los datos y generar auditorias sobre la información que se transmite.

#### 3.4.1.4 Filtros dinámicos a nivel paquete (Dynamic Packet Filters)

La cuarta generación de firewalls, llamada filtros dinámicos a nivel paquete, permite modificaciones a las reglas de seguridad sobre la marcha. En la práctica, se utilizan dos o más técnicas para configurar el firewall.

## 3.5 Medios de transmisión

Cualquier medio físico que permita transmitir información en forma de señales electromagnéticas se puede utilizar como medio de transmisión. Estas líneas de transmisión son de vital importancia, porque en ellas es donde la información fluye de un nodo a otro.

Dependiendo de la forma de conducir la señal a través del medio, los medios de transmisión se pueden clasificar en medios de transmisión guiados y medios de transmisión no guiados.

### 3.5.1 Medios de transmisión guiados

Los medios de transmisión guiados están constituidos físicamente por un cable, que se encarga de la conducción de las señales desde un punto a otro. Sus principales características son: tipo de conductor utilizado, velocidad de transmisión, distancias máximas, protección de interferencias electromagnéticas, fácil manejo e instalación, y capacidad de soportar varias tecnologías de enlace.

Dentro de estos medios de transmisión, los más utilizados en las redes Ethernet son el par trenzado, la fibra óptica y, ya casi en desuso, el cable coaxial.

#### 3.5.1.1 Par trenzado

El par trenzado consiste en dos alambres de cobre a través de los cuales fluyen las señales. El cable de par trenzado de 2 hilos es común usarlo en telefonía y transmisión de datos; puede venir de 3 o 4 pares, el empalme se realiza con conectores RJ-11 o RJ-45.

Los dos alambres de cada par trenzado están dispuestos o colocados bajo un patrón en espiral a todo lo largo de su trayectoria, porque el trenzado permite minimizar las interferencias electromagnéticas entre los cables, dado que el acoplamiento entre ellos es mayor.

Dentro de los cables de par trenzado están los cables sin blindar, llamados UTP (Unshielded Twisted Pair), y el cable blindado STP (Shielded Twisted Pair). La

diferencia entre estos dos tipos de cable es que el UTP tiene una cubierta plástica protectora, mientras que el STP tiene una malla tejida de hilos de metal.

El par trenzado tiene limitaciones para la transmisión de la señal: conforme la distancia es más grande, la señal se debilita o atenúa. Para estos casos, se necesitan repetidores, para poder regenerar y amplificar la señal nuevamente. Dependiendo de las características del cable UTP, será la distancia recomendable y máxima.

Las características de los cables de red se definen en categorías, de acuerdo con la forma y tiempo en que fueron diseñados. Se muestran algunas características de los cables UTP:

*Categoría 1:* Es el utilizado en las líneas telefónicas, adecuado para la voz, pero no para las transmisiones de datos. Las características de transmisión se especifican a una frecuencia superior a 1Mhz.

*Categoría 2:* Par trenzado UTP, su frecuencia de transmisión es superior a 4Mhz. Tiene 4 pares trenzados de hilo de cobre.

*Categoría 3:* La velocidad de transmisión es de 10Mbps para Ethernet. Se utiliza la red Ethernet 10BaseT. Frecuencia superior a 16Mhz. Tiene 4 pares trenzados de hilo de cobre.

*Categoría 4*: La velocidad de transmisión es de 20Mbps. Frecuencia superior a 20Mhz. Tiene 4 pares trenzados de hilo de cobre.

*Categoría 5:* Transmite hasta 100Mbps, con una frecuencia superior a 100Mhz. Tiene 4 pares trenzados de hilo de cobre.

*Categoría 6:* Transmite datos hasta a 1Gbps, con una frecuencia de 250Mhz. En la imagen 3.6, se muestra un cable UTP de esta categoría, utilizado en los patchcords del sistema de cableado estructurado de la DGB.

*Categoría 7:* Es una mejora de los anteriores. Transmite datos hasta a 10Gbps y tiene una frecuencia superior a 600Mhz.

En la tabla 3.1, se muestran las características principales de los cables, de acuerdo con sus categorías.

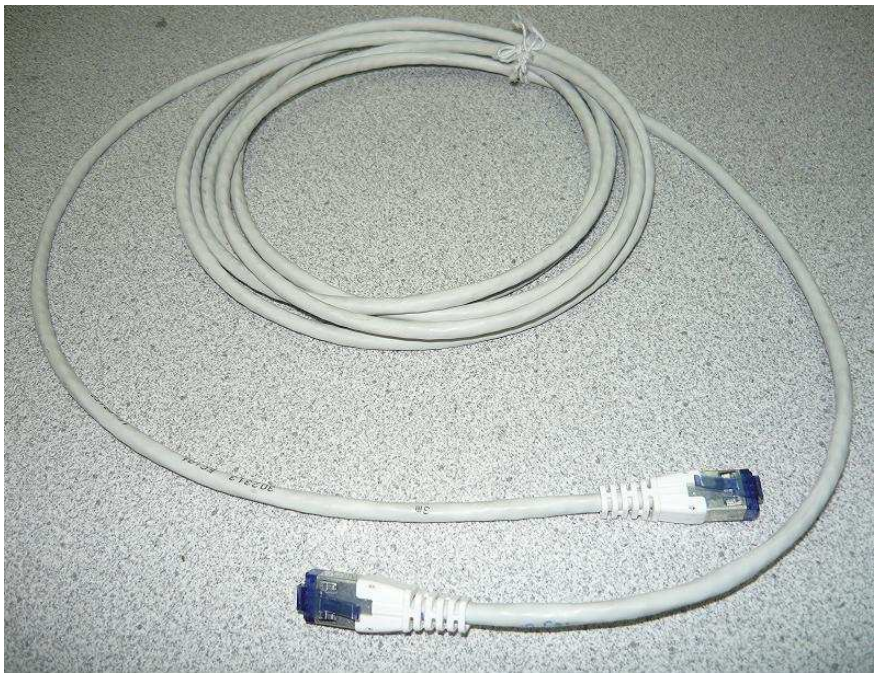


Imagen 3.6 Cable categoría 6

| Categoría | Uso | Velocidad de transmisión | Frecuencia transmisión Mhz | Pares de hilo | Distancia máxima de transmisión en metros |
|---|---|---|---|---|---|
| 1 | Telefónico | Analógico | 1 | 1 | -- |
| 2 | Descontinuado | 10Mbps | 4 | 4 | -- |
| 3 | Voz y datos | 10Mbps | 16 | 4 | 90 |
| 4 | Red LAN | 20Mbps | 20 | 4 | 100 |
| 5 | Red LAN | 100Mbps | 100 | 4 | 100 |
| 6 | Red LAN | 1Gbps | 250 | 4 | 150 |
| 7 | Red LAN | 10Gbps | 650 | 4 | No disp. |

Tabla 3.1 Características de las categorías de cable

Para las conexiones Ethernet o uniones entre 2 nodos, se utilizan conectores RJ45 y se aplican las configuraciones que se muestran en las tablas 3.2 y 3.3.

De acuerdo con la norma TIA/EIA-568-B, es el cable UTP el que se utiliza normalmente en las conexiones de una máquina hacia el nodo o rosetas. En la tabla 3.2, se muestra cómo es la relación de las conexiones para esta norma.

| Conexión 1 | Relación de pines | Conexión |
|---|---|---|
| Blanco/naranja | Pin 1 a Pin1 | Blanco/naranja |
| Naranja | Pin 2 a Pin2 | Naranja |
| Blanco/verde | Pin 3 a Pin3 | Blanco/verde |
| Azul | Pin 4 a Pin4 | Azul |
| Blanco/azul | Pin 5 a Pin5 | Blanco/azul |
| Verde | Pin 6 a Pin6 | Verde |
| Blanco/café | Pin 7 a Pin7 | Blanco/café |
| Café | Pin 8 a Pin8 | Café |

Tabla 3.2 Configuración de cable UTP

La norma TIA/EIA-568-A, es la que se refiere al par cruzado, el cual se usa para interconectar switches entre sí o dos computadoras personales. En la tabla 3.3 se muestra la relación que hay entre conexiones.

| Conexión 1 | Relación de pines | Conexión |
|---|---|---|
| Blanco/naranja | Pin 1 a Pin1 | Blanco/verde |
| Naranja | Pin 2 a Pin2 | Verde |
| Blanco/verde | Pin 3 a Pin3 | Blanco/naranja |
| Azul | Pin 4 a Pin4 | Azul |
| Blanco/azul | Pin 5 a Pin5 | Blanco/azul |
| Verde | Pin 6 a Pin6 | Naranja |
| Blanco/café | Pin 7 a Pin7 | Blanco/café |
| Café | Pin 8 a Pin8 | Café |

Tabla 3.3 Configuración de par cruzado

### 3.5.1.2 Cable coaxial

El cable coaxial está formado por dos conductores que permiten operar sobre un rango amplio de frecuencias. Se trata de un conductor cilíndrico de cobre rodeado por un aislante, que a su vez está rodeado por un conductor externo, usado como nivel de tierra, y al final cubierto por la funda exterior.

Existen dos tipos de cable coaxial para redes locales: el primero es de 75 Ohms, estándar en los sistemas CATV, que es usado para señal analógica. El segundo cable es el de 50 Ohms, conocido como banda base, que es un medio rápido pero de un solo canal. Se usa sólo para transmisión digital. Ver imagen 3.7.

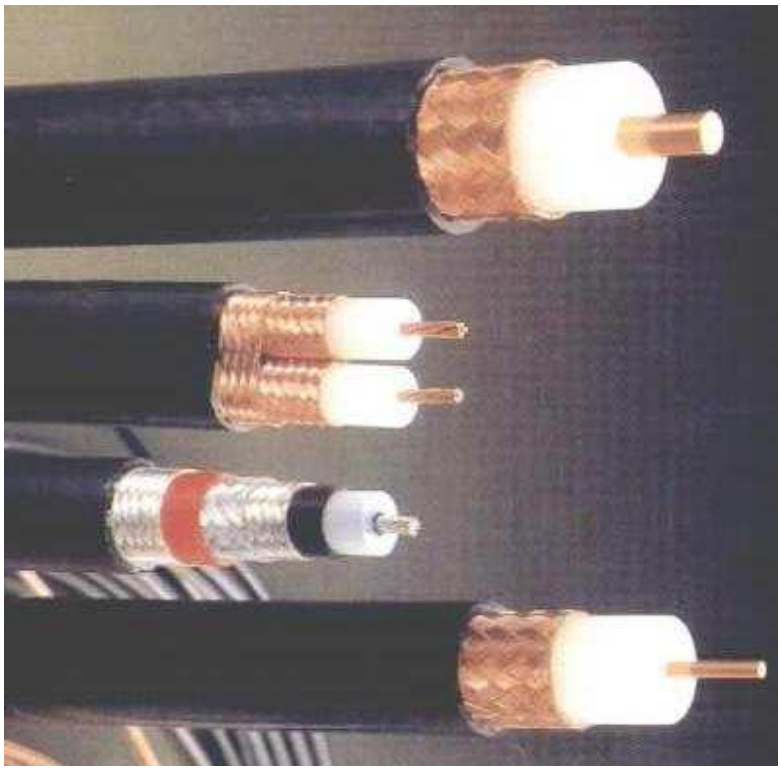


Imagen 3.7 Cable coaxial

Las distancias máximas de transmisión sin necesidad de repetidores, es para el cable de 75 Ohms de 600m, para cables de 50 Ohms de 0.2 pulgadas de 300m, y de 0.4 pulgadas de 500m.

A causa de la necesidad de manejar frecuencias más altas y la digitalización de las transmisiones, en los últimos años se ha ido sustituyendo paulatinamente el uso del cable coaxial por el de fibra óptica, en particular para distancias superiores a varios kilómetros, porque el ancho de banda de ésta última es muy superior.

### 3.5.1.3 Fibra óptica

Una fibra óptica, dentro del concepto de red, es un medio flexible de dimensiones reducidas por el cual pasa la luz. Las fibras ópticas son fabricadas con diferentes plásticos y cristales.

La fibra óptica es una delgada fibra de vidrio o silicio fundido que conduce la luz, en la cual se requieren 2 filamentos para una comunicación bidireccional: TX y RX. Su grosor va de 50 a 125 micrómetros de diámetro.

En la imagen 3.8 se ve una fibra óptica multimodo con conectores ST y SC-dúplex, que se utilizaba en la DGB.

Imagen 3.8 Fibra óptica

En los filamentos de la fibra óptica se tiene la fuente de luz, que es el led o láser, el medio en que se transmite, que es la fibra óptica, y el detector de la luz o señal enviada, que es el fotodiodo. De manera general, el cable de fibra óptica está cubierto por núcleo, manto, recubrimiento, tensores y chaqueta. En este caso, la señal es enviada mediante pulsos de luz. El 1 indica un pulso de luz y el 0 ausencia de luz.

Existen tres tipos de fibras ópticas:

- La fibra multimodal de índice de refracción escalonado, que es utilizada en la transferencia convencional de imágenes, y en la transmisión de datos en distancias cortas.

- La fibra multimodal de índice de gradiente, en la cual el índice de refracción del núcleo disminuye gradualmente del centro hacia fuera; es óptima para las distancias intermedias.

- La fibra monomodo; está diseñada para largas distancias y gran velocidad en la transmisión de datos, con poca diferencia de índice de refracción y núcleo de tamaño pequeño.

La capacidad de transmisión de información depende básicamente de tres características: el diseño geométrico de la fibra, las propiedades de los materiales empleados (diseño óptico) y el intervalo de longitudes de onda de la fuente de luz

utilizada (cuanto mayor sea éste, menor será la capacidad de transmisión de información de la fibra). En la imagen 3.9 se dan las características principales de los tipos de transmisión de la fibra óptica.

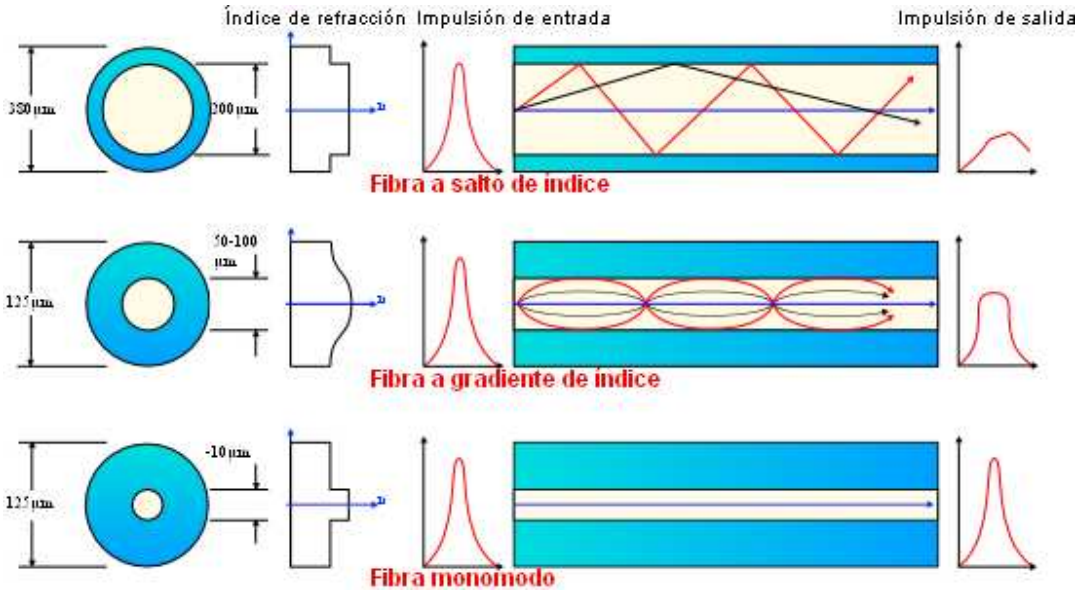



Imagen 3.9 Tipos de transmisión de fibra óptica

*Fast Ethernet*

Las normas Fast Ethernet para fibra óptica fueron aplicadas en la década de los 90, todas las Ethernet a 10Mbps instaladas se habían actualizado a 100Mbps o Fast Ethernet.

Las normas de fibra para Fast Ethernet 100Base-FX incluyen 100Base-SX y 100Base-BX.

- 100Base-FX utiliza una luz a 1300nm multimodo. La longitud máxima de transmisión es de 2 kilómetros para dúplex completo, a través de esta fibra óptica multimodo.

- 100Base-SX es la alternativa de menor costo a 100Base-FX. Utiliza 850nm, pero sólo puede operar a una distancia de hasta 300 metros. Evidentemente, según la aplicación, es más que suficiente.

- 100Base-BX es la versión de Fast Ethernet a través de un solo hilo de fibra óptica. (Ambos, 100Base-FX y 100Base-SX usan dos líneas de fibra óptica). Esta tecnología utiliza WDM (multiplexación por división de longitud

de onda) como tecnología para separar la transmisión y la recepción de señales.

*Gigabit Ethernet*

A finales del decenio de 1990 y principios de 2000, la mayoría de las 100Mbps Fast Ethernet instaladas se actualizaron a 1000Mbps, o también llamado Gigabit Ethernet. En el mismo proceso, la fibra es cada vez más el medio de transmisión de elección cuando el cobre alcanza sus límites fundamentales para la transmisión de alta velocidad.

Para transceptores de fibra óptica, los estándares de la industria relacionados incluyen 1000Base-SX, 1000Base-LX, 1000Base-LH, 1000Base-BX10 y 1000Base-ZX.

- 1000Base-SX utiliza 850nm multimodo sobre fibras multimodo. Sus especificaciones dicen que la longitud máxima de operación es de 500 metros, pero, por lo general, puede llegar a mucho más que eso.

- 1000Base-LX funciona a 1300 o 1310nm con fibra monomodo. Sus especificaciones dicen que la longitud máxima de operación es de 5 kilómetros, pero los fabricantes a menudo garantizan más de 10 kilómetros de longitud de trabajo.

- 1000Base-LH no es un estándar, pero es muy aceptada por la industria. Es compatible con 1000Base-LX, pero su especificación está en 10 kilómetros sobre fibra monomodo. Esto realmente se logra utilizando componentes de muy alta calidad en fibra óptica.

- 1000Base-BX10 opera en un solo hilo de fibra monomodo. Similar a 100Base-BX, transmite mediante la tecnología WDM. Su especificación se encuentra en 10 kilómetros de distancia de transmisión.

- 1000Base-ZX tampoco es un estándar de la industria, pero vuelve a ser una normativa muy aceptada por la industria. Utiliza 1550nm mediante fibra monomodo para operar en distancias de hasta 70 kilómetros.

*10 Gigabit Ethernet*

10 Gigabit Ethernet también se denomina 10GigE. Esta normativa fue publicada por primera vez en 2002 y sigue siendo el estándar Ethernet más rápido, aunque 100Gbit Ethernet está ya en desarrollo. El estándar incluye 10GBase-SR, 10GBase-LR, 10GBase-LRM, 10GBase-ER, 10GBase-ZR y 10GBase-LX.

## 3.6 Cableado estructurado

En este punto se hace referencia al cableado estructurado que se ha hecho en la Biblioteca Central como antecedente y base sobre la cual la tesis se fundamentó, ya que sin el cableado estructurado realizado con anterioridad no se hubiera podido realizar o hubiera sido demasiado difícil alcanzar.

Antes de 1985, no se tenían estándares para aplicar el cableado estructurado, cada fabricante de equipo realizaba sus propios “estándares”. Cada cambio de equipamiento de cómputo también incluía el cambio del sistema de cableado, que resultaba costoso. Posterior a este año, se generaron recomendaciones que se convertirían en estándares.

Estos estándares definieron el cableado estructurado como un sistema de cables, conectores, espacios, etiquetas, canalizaciones y demás dispositivos que deben ser instalados para poder establecer o diseñar una infraestructura de comunicaciones de manera general en un edificio, campus o área de trabajo con necesidades de comunicación grandes. Todo esto debe estar apegado a los estándares definidos para el cableado estructurado, para que sea reconocido como tal.

La instalación, al estar acorde con los estándares establecidos para el cableado estructurado, trae consigo los beneficios de independencia de proveedor y protocolo, flexibilidad de instalación, capacidad de crecimiento y facilidad de administración. Este cableado estructurado se realiza con la finalidad de tender los cables en el interior de la construcción, con el propósito de implantar una red local, o en nuestro caso mejorarla. Por lo regular se utiliza el cable UTP para redes de tipo Ethernet, aunque también se hace con fibra óptica o cable coaxial.

El cableado principal se puede separar en 3 zonas de trabajo, que se mencionan en los siguientes apartados.

### 3.6.1 El cableado horizontal o de planta

El cableado horizontal o de planta es el que se encuentra en un mismo nivel del edificio y se concentra en el clóset o armario de telecomunicaciones. En este clóset se realizan todas las conexiones o empalmes de unos cables con otros; de acuerdo con el diseño, se puede colocar equipo activo para concentrar el sistema de cableado, como son los switches, hubs, servidores proxy o algún otro dispositivo necesario.

Esta zona comprende el conjunto de medios de transmisión, como son los cables o las fibras que unen los puntos de distribución con los conectores del puesto de trabajo. Es muy importante ver esta parte al momento del diseño, ya que los

puntos de conexión en el sistema de cableado varían mucho, de acuerdo con las necesidades de servicio del nivel del edificio donde se encuentre.

En la imagen 3.10 se puede ver el tipo de cableado estructurado del tipo horizontal descrito.

Imagen 3.10 Sistema de cableado estructurado tipo horizontal

### 3.6.2 El cableado vertical, troncal o backbone

El cableado vertical, troncal o backbone es la zona donde se conectan uno o más clósets de telecomunicaciones mediante otro conjunto de cables que atraviesan verticalmente el edifico de nivel a nivel. Se realiza mediante canalizaciones existentes en el edificio, o se habilitan nuevas canalizaciones, o se utilizan espacios existentes, como elevadores, escaleras o por fuera del edificio; éste último no es recomendable.

Esta zona tiene la función de red troncal y junta el consumo de ancho de banda del cableado horizontal; por ende, se utiliza o debe utilizarse tecnología de mayor capacidad, o en su caso el mismo tipo, pero teniendo en consideración una correcta distribución del ancho de banda.

En la imagen 3.11, se ve la característica principal del sistema de cableado del tipo vertical que atraviesa los pisos de la Biblioteca Central para conectar los backbones.


Imagen 3.11 Cableado vertical

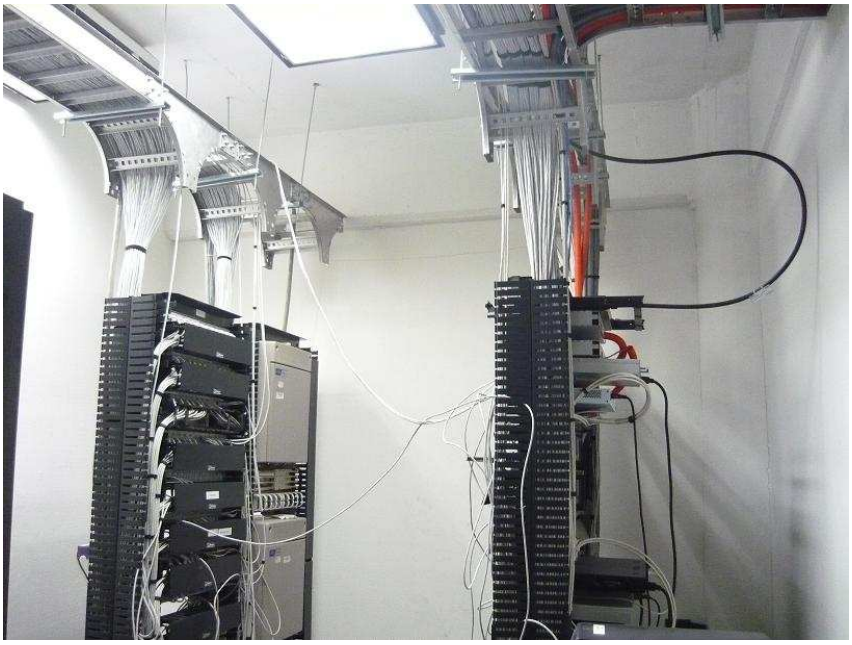


Imagen 3.12 Cuarto principal

### 3.6.3 El cuarto principal de equipos y de entrada de servicios

El cableado vertical y el horizontal terminan en una sola acometida, donde se concentran y terminan las conexiones del edificio para finalmente salir al exterior. En este punto se concentra en su mayor parte la infraestructura de telecomunicaciones, tales como las puertas de enlace, el firewall, la central telefónica y, si se tiene suficiente espacio, el área de servidores.

En la imagen 3.12, se ve el cableado central en el cuarto principal de la DGB, que es el punto de conexión de la LAN hacia el exterior.

### 3.6.4 Estándares para cableado estructurado

#### 3.6.4.1 TIA/EIA-569-B Commercial Building Standard for Telecommunications Pathways and Spaces

Espacios y canalizaciones para telecomunicaciones en edificios comerciales.

Provee especificaciones para el diseño de las instalaciones y la infraestructura necesaria para el cableado de telecomunicaciones en edificios comerciales.

Cuenta con tres conceptos fundamentales, relacionados con telecomunicaciones y edificios: Los edificios son dinámicos, los sistemas de telecomunicaciones son dinámicos y las telecomunicaciones son más que “voz y datos”. Además de que identifica componentes para trabajar: Las instalaciones de entrada, la sala de equipos, el backbone, clósets de comunicaciones, canalizaciones horizontales y áreas de trabajo.

#### 3.6.4.2 J-STD-607-A Commercial Building Grounding (Earthing) and Bonding Requirements for Telecommunications

Tierras y aterramientos para los sistemas de telecomunicaciones en edificios comerciales.

En este documento se brindan los criterios de diseño e instalaciones de tierras y sistemas de aterrizaje o aterramiento para edificios comerciales, con o sin conocimiento previo acerca de los sistemas de telecomunicaciones que serán instalados. Incluye recomendaciones respecto a las tierras y sistemas de aterramiento para las torres y antenas. Prevé edificios compartidos por varias empresas y ambientes con diversidad de productos de telecomunicaciones.

### 3.6.4.3 TIA/EIA-568-B de alambrado de telecomunicaciones para edificios comerciales, requerimientos generales, componentes de cableado de par trenzado

Este estándar y sus correspondientes actualizaciones, hasta 2006, establecen los requerimientos de un sistema integral de cableado que sea independiente de las aplicaciones y de los proveedores para los edificios comerciales. Se estima que el tiempo de vida productiva del cableado estructurado debe ser de 15 a 25 años, debido a la tendencia de las tecnologías, que están cambiando conforme el transcurso del tiempo, y por ende se deben tomar en cuenta los futuros cambios de ancho de banda, conforme la demanda de datos que crece con el tiempo y que debe soportar las tecnologías actuales y futuras.

Se especifican los requerimientos mínimos para cableado estructurado de telecomunicaciones dentro de un ambiente de oficina, para distintas tecnologías de cables (cobre y fibra), las topologías y distancias recomendadas, y los parámetros de comportamiento de los medios de comunicación, como el cobre y la fibra.

En este estándar, los documentos EIA-568-B.1 y EIA-568-B.2 corresponden a sistemas de cableado estructurado alámbrico. El EIA-568-B.3 habla sobre las características de los componentes y parámetros de transmisión en un cableado basado en fibra óptica.

### 3.6.4.4 TIA/EIA-606-A Administration Standard for Commercial Telecommunications Infrastructure

Administración estándar para la infraestructura de telecomunicación comercial. Subsistema de administración.

Con el fundamento que se tiene al respecto sobre un edificio que tiene un tiempo de vida útil de 50 años, el continuo movimiento de personal, implementación y retiro de servicios, y a sabiendas de que el mantenimiento de los registros administrativos desempeña un papel necesario para saber las condiciones del sistema de cableado, se definieron normas para apoyar la documentación de rutas y trayectorias del mismo cableado.

En esta norma:

- Se definen conceptos administrativos, como expedientes, informes, planos y órdenes de trabajo.

- Se establecen identificadores, como números únicos a cada punto de terminación del cable y tierra.

- Se elaboran expedientes de las telecomunicaciones, en los que se indica la ubicación del cable, el espacio que ocupan, la ruta a seguir, las conexiones a tierra y la ubicación de la terminación y hardware que se utiliza.

- Se agregan los acoplamientos o registros adicionales que sirvan de ayuda para una mejor identificación del hardware y cableado, como el modelo de hardware, inventarios, claves de acceso y la ubicación de PBX. Asimismo, se establece algún código alfanumérico para identificar rápido la ubicación de cada pieza.

# CAPÍTULO 4

# ANÁLISIS Y DISEÑO

## 4.1 Estructura de la red Ethernet

Desde el año 2000, la red Ethernet del edificio de la Biblioteca Central, conformada por una topología de estrella, se desarrolló bajo el concepto de sistema de cableado estructurado, en un principio con categoría 5. En 2005, cuando empezó la renovación del cableado estructurado, se utilizó cable categoría 6. Este sistema de cableado cuenta con un cuarto principal llamado MDF (Main Distribution Frame), con acometidas de fibra óptica hacía el exterior y conectando también con los cuartos secundarios o IDF's (Intermediate Distribution Frame), a través del backbone, manteniendo la comunicación entre ellos mediante switches.

El sistema principal de comunicaciones MDF se ubica en el nivel Basamento y se tienen seis IDF's en diferentes niveles del edificio.

Los cuartos de comunicación, ubicados en el backbone, como el cuarto principal, cuentan con un sistema de tierras físicas, independiente de las demás áreas de trabajo de la Biblioteca Central; tienen condiciones adecuadas de temperatura mediante aire acondicionado y soportados por UPS (Uninterrumpted Power System), para prevenir contingencias eléctricas.

Una muestra de los aires acondicionados y los UPS se puede ver en las imágenes 4.1 y 4.2, ubicados en el área de backbone y servidores, respectivamente.

Imagen 4.1 Sistema de aire acondicionado

Imagen 4.2 UPS

Para la cuestión de seguridad, se tiene en cuenta un firewall en el punto de intercambio de datos entre la red local y el exterior, así como un firewall que sirve para filtrado de correo electrónico.

En el MDF se hace la distribución y administración de la red mediante el equipo principal: un switch Extreme Alpine 3880 que tiene tarjetas de expansión para conectar fibra o UTP. En todos los cuartos de comunicación se tienen switches, distribuidos de tal forma que cubren la demanda de los nodos de comunicación.

Se puede ver de forma gráfica, en la imagen 4.3, la distribución de los IDF en los backbones y la conexión hacia el cuarto principal.

A excepción del rack en piso 10, la demanda soportada conforme a la cantidad de nodos en el MDF y cada IDF es de 60% a 100%, y va cambiando conforme se realizan movimientos de personal o se van implementando nuevos servicios.

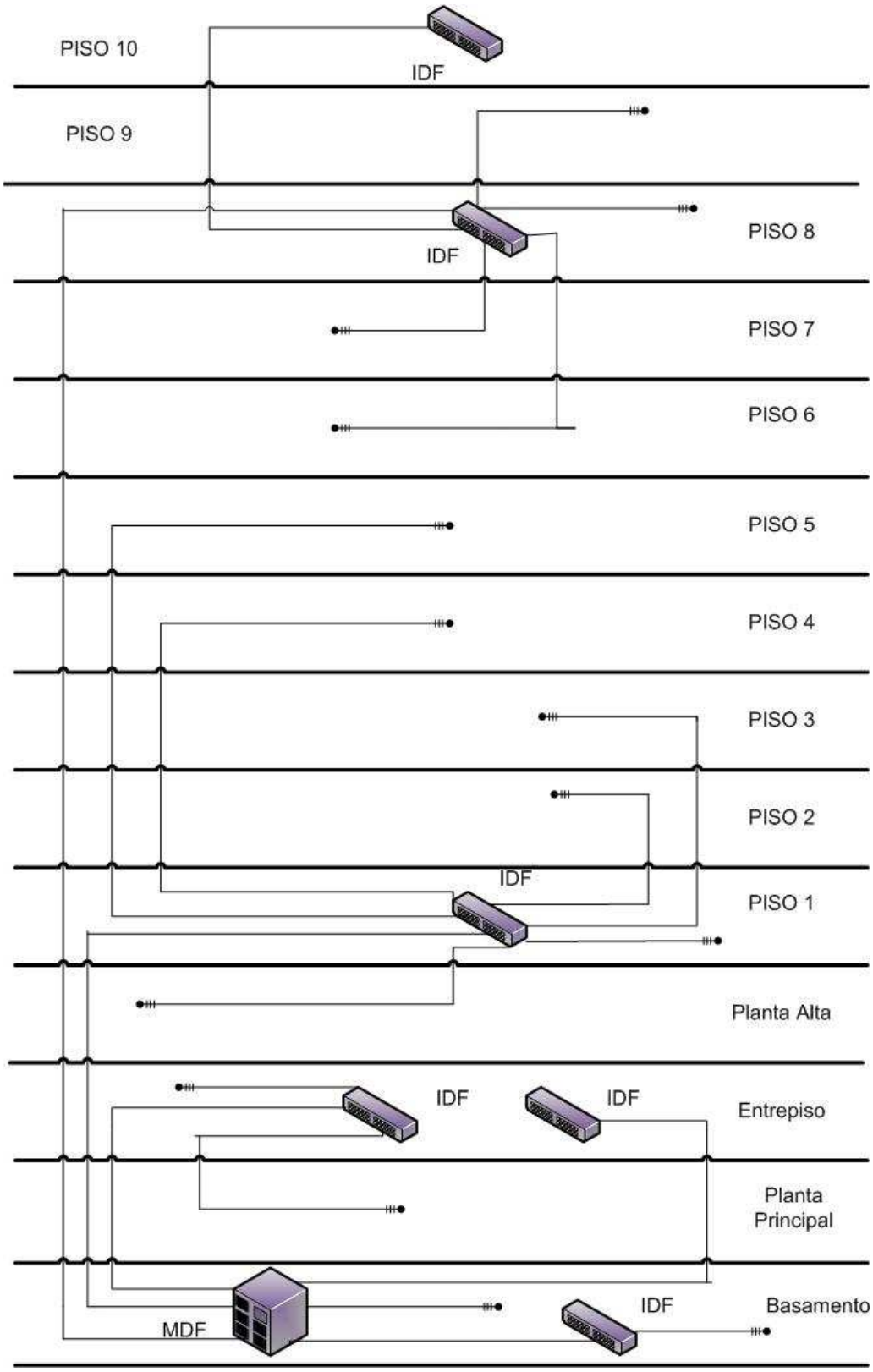



Imagen 4.3 Distribución de los cuartos de comunicación

Debido a que se tienen grandes cantidades de nodos y switches presentes en los cuartos de comunicación de la Biblioteca Central, se ha tenido cuidado con el manejo de éstos, identificando cada nodo para su respectiva administración y documentación mediante memorias técnicas y manejo del sistema de inventario de los equipos que tiene la Biblioteca Central.

Respecto a la planeación para la instalación de los nodos, y conforme ha pasado el tiempo, se ha considerado tener determinada cantidad de nodos, como se muestra en la tabla 4.1, la cual muestra los nodos realizados con cable categoría 6. Cabe mencionar que en el año 2000 se había llegado a la cantidad de 461 nodos planeados, pero en categoría 4; posteriormente se sustituyó por la categoría 6.

A la fecha, los nodos se han ido incrementando y ya casi no hace falta habilitar nodos con cableado categoría 6; estos nodos son los mínimos, de acuerdo con el proyecto de renovación de cableado. También se ha considerado que se llegará a un límite de nodos, dada la capacidad de la BC en cuanto a espacios, por lo que el aumento de nodos prácticamente no pasará de lo planeado.

| Año | Nodos planeados para instalar, pensando en categoría 6 desde el año 2004 | Nodos instalados |
|---|---|---|
| 2005 | 570 | 512 |
| 2007 | 803 | 788 |
| 2009 | 960 | 944 |
| Agosto 2010 | 970 | 964 |
| Tendencia hacia el año 2011 | 970 | -- |

Tabla 4.1 Nodos planeados e instalados

## 4.2 Servicios en la DGB y BC

La Biblioteca Central proporciona servicios de atención a usuarios y a las bibliotecas dependientes de la Dirección General de Bibliotecas. En cuestión de informática, proporciona servicios importantes, como son:

- Internet
- Correo electrónico institucional
- Servicios de videoconferencia
- Consulta automatizada de catálogos de las diferentes bases de datos de la DGB. En la imagen 4.4 se muestra la página principal de la DGB con los estándares establecidos por DGSCA

- Accesos de manera remota de las 143 bibliotecas a las bases de datos de la DGB
- Servicio de Red Inalámbrica Universitaria (RIU)

La tecnología Ethernet utilizada en la BC es Fast Ethernet y Gigabit Ethernet.


Imagen 4.4 Página web de la DGB

El consumo de ancho de banda al día varía conforme la demanda, tanto de usuarios como del personal que trabaja en la dependencia y sus necesidades de trabajo.

En la parte de los servicios al usuario, lo más utilizado por ellos son los catálogos automatizados de las diferentes bases de la DGB y BC, el préstamo electrónico de libros, la modalidad de auto préstamo y el servicio de renta de computadoras que se ofrece en el departamento de Consulta. El servicio de préstamo de libros tiene gran afluencia durante los fines de semana, por lo que se tienen los equipos trabajando al 100%, dado que hay filas para poder consultar los catálogos.

El personal de la DGB, es el que principalmente utiliza Internet, junto con el departamento de Consulta, utilizando el ancho de banda de manera variable, de acuerdo con los servicios que se estén ofreciendo o solicitando en esos momentos. Se muestra una gráfica sobre el consumo de ancho de banda en la BC, mediante el programa Firewall Analyzer 6, que actualmente se está utilizando para esos fines, en la imagen 4.5.

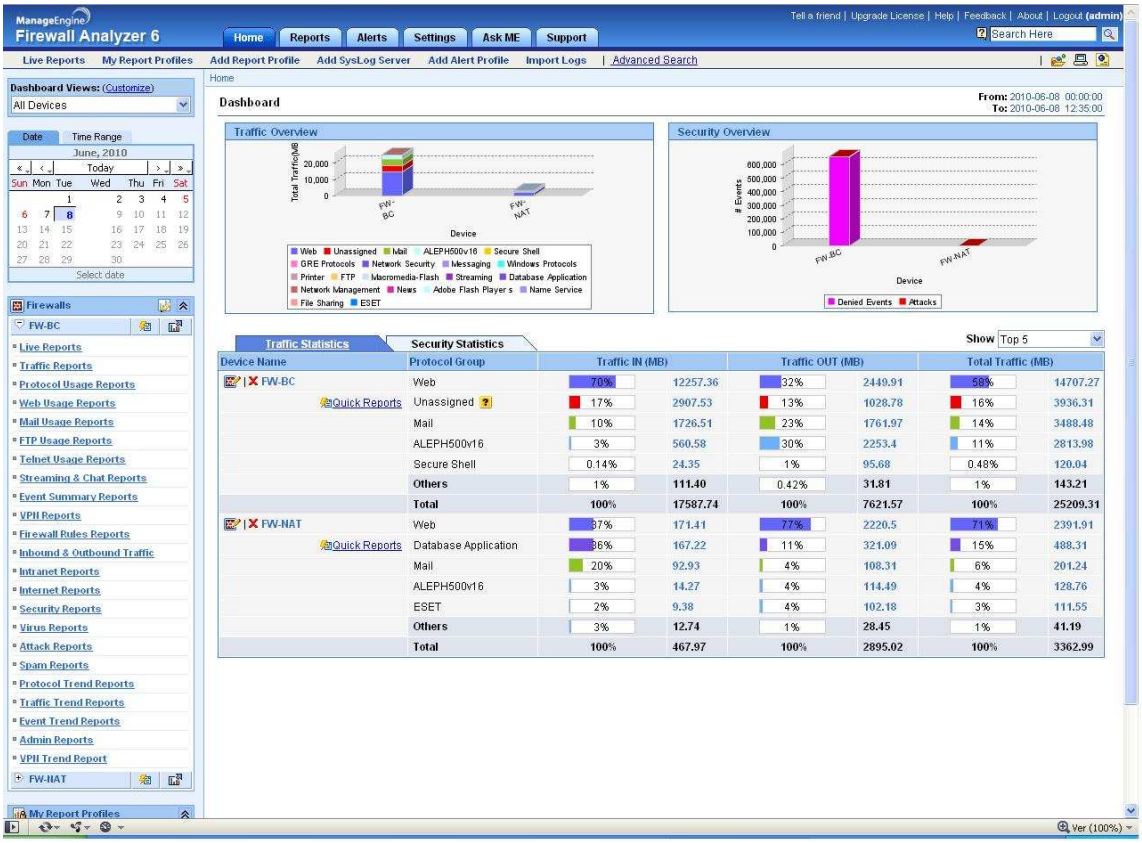



Imagen 4.5 Captura de estadísticas de tráfico con Firewall Analyzer 6

El sistema de cableado estructurado, como está recién instalado y acorde con las normas, reúne los requisitos para tener una vida óptima de diez años o un poco más. Respecto a su crecimiento, ya tendrá poco que incrementarse, porque están prácticamente cubiertos los nodos necesarios en BC.

## 4.3 Equipos en servicio

La cantidad de computadoras y equipo activo que se están utilizando, en su mayoría, han sido adquiridos dentro del periodo de medio año a cinco años, siendo las computadoras principalmente de la marca Dell, de diferentes modelos, las impresoras marca HP, laptops marca Toshiba, switches marca Extreme y 3Com, y servidores marca SUN.

En la tabla 4.2, se muestra una relación de los equipos en red de los que disponía la Biblioteca Central a finales de los años 2005, 2006, 2007 y 2009. Los datos fueron tomados de los censos anuales que realiza la DGB.

| Equipo | 2005 | 2006 | 2007 | 2009 |
|---|---|---|---|---|
| PC | 387 | 410 | 437 | 485 |
| Laptops | 45 | 45 | 45 | 49 |
| Impresoras sin red | | | | 48 |
| Impresoras con adaptador de red | 40 | 45 | 53 | 58 |
| Switch | 21 | 28 | 38 | 56 |
| Firewall | 1 | 1 | 1 | 3 |
| Acces Point | 2 | 2 | 3 | 15 |
| Servidores | 25 | 25 | 27 | 31 |
| | | | | |
| Total | 521 | 556 | 610 | 697 |

Tabla 4.2 Cantidad de equipos disponibles en red en diferentes años

Para lo que nos interesa, estamos refiriéndonos a 697 equipos con capacidad de conectarse a la red de la BC. Si se confronta con la cantidad de nodos disponibles, que son 944, son más que suficientes para controlar la demanda e incrementos de nuevos servicios.

En la tabla 4.3, se muestra una lista más desglosada de la cantidad de equipos de que se disponían hasta principios del año 2010, donde aparece la cantidad de equipos disponibles por departamento, el tipo de procesador que tienen y las impresoras disponibles. Como puede observarse, la envergadura de la infraestructura tecnológica, así como la diversidad de áreas y departamentos, es grande.

| Área | PC´s actuales | | | | | | | Impresoras - Escáneres actuales | | | | | | | | | | | | | Otras impresoras | | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | *P-III* | *P-IV* | *P-D* | *P-C* | *lap* | *Sup o MAC* | *Total* | *Escáner* | *IV* | *1110* | *2100* | *2200* | *2300* | *2420* | *4250* | *4050* | *4550* | *p4015* | *8250* | *Otros* | Multif. | Otras | |
| **Dirección** | | 2 | 3 | | 1 | 1 | 7 | 1 | | | | 2 | | 1 | | | | | | 1 | | | 4 |
| Publicaciones | 1 | 2 | 2 | | | 3 | 8 | 1 | | | | | | | 1 | | 1 | | | | 1 | | 3 |
| **Subdirección de Biblioteca Central** | | 1 | 1 | | 27 | | 29 | | | | | 2 | | | | | | | | | | 1 | 3 |
| Circulación Bibliográfica y Turno Especial | | 53 | 5 | | | | 58 | | | | | 1 | | 1 | | | | | | | | 9 | 11 |
| Consulta | | 50 | 8 | 2 | 1 | | 61 | 3 | | | | | | 1 | 1 | | | 2 | | | | 1 | 5 |
| Publicaciones periódicas | | 12 | 5 | 2 | | | 19 | 1 | | 1 | | 2 | | | | | | | | | | | 3 |
| Selección y Adquisición Bibliográfica | | 3 | 11 | 2 | | | 16 | | 1 | | | | | | 1 | 2 | | | | 1 | | 1 | 6 |
| Tesis | | 17 | 11 | 1 | | | 29 | 4 | | | | 1 | | | 2 | | | | | 2 | | | 5 |
| Fondo Antiguo | | 4 | 10 | | | | 14 | 1 | | | | | | | 1 | | | | | | | | 1 |
| **Subdirección de Informática** | | 1 | 2 | | 1 | | 4 | | | | | | | | 1 | | | | | 1 | | | 2 |
| Sistemas | | 3 | 13 | 3 | 4 | 2 | 25 | | | | | | | 1 | 1 | | | | | 2 | | | 4 |
| Producción | | 1 | 14 | 4 | 8 | | 27 | | | | | | | | | | | | | | | 3 | 3 |
| Producción IDFs-MDF | | 5 | 1 | | | | 6 | | | | | | | | | | | | | | | | 0 |
| Producción Stock | | 24 | 8 | | | | 32 | | | | | | | | 2 | | | | | | | 10 | 12 |
| Producción Sala fría | | 1 | 5 | | | 1 | 7 | 1 | | | | | | | | | | 1 | | | | | 1 |
| Videoconferencia | | | 2 | | 2 | | 4 | | | | | | | | | | | | | | | | 0 |
| **Subdirección de Planeación y Desarrollo** | | 1 | | 1 | | | 2 | | | | | | | | 1 | | | | | | | 1 | 2 |
| Desarrollo de Personal | | 4 | 29 | | | | 33 | 1 | 1 | | | 3 | | | 1 | | | | | | | | 5 |
| Planeación | | 6 | 7 | | | | 13 | | | | | 2 | | | | | | | | | | | 2 |
| **Secretaría Académica** | | 2 | 3 | 2 | 1 | | 8 | 1 | | | 1 | 1 | | | | | | | | | 1 | | 3 |
| Educación Continua | | 1 | 1 | 1 | | | 3 | | | | | | | | 1 | | | | | | 1 | | 2 |
| **Unidad Administrativa** | | 1 | 2 | | 1 | | 4 | | | | | | | | 1 | | | | | 1 | | | 2 |
| Compras, Almacén e Inv. | 1 | 3 | 1 | 1 | 2 | | 8 | 2 | | 1 | | 1 | | | | | | | | 1 | 1 | | 4 |
| Contabilidad y Presup. | 1 | 4 | 1 | | | | 6 | | | | | 1 | | | 1 | | | | | | | | 2 |
| Personal | 1 | 3 | | | | | 4 | | | 1 | | 1 | | | | | | | | | | | 2 |
| Servicios Generales | | 3 | 1 | | | | 4 | | | | | | | | | | | | | 1 | | | 1 |
| Campañas de FUNDACIÓN UNAM | | 2 | | | | | 2 | | | | | | | | | | | | | | | | 0 |
| Correspondencia | 1 | | | | | | 1 | | | | | | | | | | | | | | | | 0 |
| Imprenta | | 1 | | | | | 1 | | 1 | | | | | | | | | | | | | | 1 |
| Sindicato | | | 2 | | | | 2 | | | | 1 | | 1 | | | | | | | | | | 2 |
| **Subdirección Técnica** | | 2 | | | 1 | | 3 | | | | | 1 | | 1 | | | | | | | | | 2 |
| Procesos Técnicos | | 26 | 7 | 6 | | | 39 | | | | | 4 | | 1 | 1 | | | | | | | | 6 |
| Adquisiciones | | 2 | 7 | 6 | | | 15 | | | | 1 | 1 | | 1 | 1 | | | | | 1 | | | 5 |
| Catálogo Colectivo | 1 | 8 | | | | | 9 | | | | | | | 2 | | | | | | | | | 2 |
| Restauración | 1 | | | | | | 1 | | | 1 | | | | | | | | | | | | | 1 |
| | | | | | | | | | | | | | | | | | | | | | | | |
| **TOTALES** | **7** | **248** | **162** | **31** | **49** | **7** | **504** | **16** | **3** | **4** | **3** | **23** | **1** | **9** | **17** | **2** | **1** | **3** | **0** | **11** | **4** | **26** | **107** |
| | | | | | | | 504 | | | | | | | | | | | | | | | 107 | |

Tabla 4.3 Computadoras e impresoras contadas durante el censo de equipo de cómputo, enero de 2010

## 4.4 Planeación de la segmentación de la red

La segmentación de la red consiste en separar una red en varias redes diferentes, apoyándonos en las propiedades que tienen las redes privadas y mediante la utilización de dispositivos físicos o lógicos que se tienen desarrollados para este fin.

La red de la Biblioteca Central tiene a su disposición un segmento de red 132.248.67.0, con el cual, al no ser suficiente para la cantidad de equipos, se ha tenido que buscar solución para dar el servicio, para lo cual se planeó realizar la segmentación para resolver este problema. Se define que se tienen que registrar las direcciones MAC e IP que se van a utilizar en este proceso de cambio de IP.

Con la implementación del cableado estructurado categoría 6 en el edificio de la Biblioteca Central, se ha logrado tener mejor organizados y administrados los cuartos de control, así como las ubicaciones de los nodos y el conocimiento de cuántos equipos en realidad se conectan o se pueden conectar en cada departamento.

Apoyándonos en el cableado estructurado, y debido a los servicios de Internet e Intranet que se ofrecen, se decidió segmentar la red de la BC para cubrir esas necesidades.

Lo que se tiene planeado con esta segmentación es brindar una comunicación más eficiente, teniendo del lado del usuario tiempos de respuesta más cortos respecto a los servicios requeridos, y del lado del administrador un mejor control sobre lo que está transmitiendo cada equipo para, en su caso, poder identificar el problema más rápido si lo hubiera.

Para el manejo de la red, se pretende tomar segmentos de la red privada 192.168.X.X de clase C, definidos principalmente por departamentos, y en el caso de que el departamento abarque diferentes áreas o niveles del edificio, tratar de comunicarlos con el mismo segmento.

Exceptuando los equipos del área de la Dirección, la Subdirección de Informática y los dispositivos que por la naturaleza del servicio que prestan requieren de una IP pública, como son los switch, firewall, firewall spam y servidores, se tiene pensado ingresarlos a este tipo de red privada.

## 4.5 Software requerido OpenBSD

Se decidió utilizar el sistema operativo OpenBSD, que es un sistema operativo libre multiplataforma orientado a la portabilidad, estandarización, seguridad y criptografía. El software es de carácter gratuito y sus requerimientos de hardware son mínimos.

Se muestra la tabla 4.4 con los procesadores que soporta este operativo:

| |
|---|
| 80486 (DX/DX2/DX4) |
| Intel Pentium/Pentium-MMX |
| Intel Pentium Pro/II/III/Celeron/Xeon |
| Intel Pentium 4/D |
| Intel Pentium M |
| Intel Core |
| Intel Core 2 (Véase también OpenBSD/amd64 for 64-bit support) |
| Intel Atom |
| AMD 5x86 |
| AMD K5/K6/K6-2/K6-3 |
| AMD Athlon/Duron/Sempron |
| AMD Athlon 64/Opteron/Turion/Phenom (Véase también OpenBSD/amd64 for 64-bit support) |
| Cyrix MediaGX/M1/M2 |
| Cyrix 6x86 |
| VIA C3/C7 |
| Rise mP6 |
| IDT WinChip and C3 |
| NexGen 586 |
| NS Geode GX1 and M1 |
| AMD Geode GX/LX/NX |
| Transmeta TMS3200, TMS5400, TMS5600 |

Tabla 4.4 Procesadores soportados por OpenBSD

El objetivo de utilizar el OpenBSD es darle a los segmentos privados acceso a la red mediante Network Address Translation (NAT) mediante políticas de acceso vía software del que dispone el sistema operativo. Este operativo se denomina packet filtering o filtrado de paquetes.

## 4.6 Hardware requerido

Dadas las características del sistema operativo OpenBSD, se puede utilizar equipo que cuente con procesador Pentium. Para nuestro caso, tenemos a nuestra disposición equipos con plataforma Intel marca Dell, que trabajan con procesadores Pentium IV y Pentium D. La cantidad de memoria que oscila en estos equipos va de 256Mb a 1Gb.

El costo por invertir en nuevo hardware para este proyecto respecto a computadoras es nulo, debido a que ya se tiene adquirido, en este caso, equipo ya disponible en la biblioteca. Lo que tiene costo son las tarjetas de red adicionales que tendría cada equipo (por lo menos, 3 tarjetas más de red).

Respecto al equipo activo, como son los switch, si se requiere adquirir más unidades, serían las mínimas, dado que la infraestructura de equipo activo ya está en uso y funcional.

En este caso, la factibilidad operacional de los equipos depende de cómo interactúe con el operativo. Se realizaron pruebas de instalación, comunicación de red, configuraciones de políticas y de rendimiento en la red en varios modelos de equipos disponibles en ese momento, resultando todas con resultados positivos.

Las características generales de los equipos que se utilizaron para las pruebas fueron los siguientes:

A) CPU Dell Precision WS370
   Procesador Pentium IV Prescott Dt 3.2Ghz
   Memoria de 512Mb en RAM
   Tarjeta de video Nvidia
   Conexiones USB para teclado y mouse
   Tarjeta Fast Ethernet 10/100 integrada

B) CPU Dell Dimension 5150
   Procesador Pentium D 2.8Ghz
   Memoria de 512Mb en RAM
   Tarjeta de video ATI Radeon
   Conexiones USB para teclado y mouse
   Tarjeta Fast Ethernet 10/100 integrada

C) CPU Dell Dimension 4700
   Procesador Pentium IV 2.8Ghz
   Tarjeta de video Nvidia
   Conexiones minidim para teclado y mouse
   Tarjeta Fast Ethernet 10/100 integrada

Se decidió utilizar el equipo WS Precision 370, principalmente, por la cantidad de puertos PCI que tiene disponibles: 4 puertos PCI para conectar tarjetas 10/100/1000 de red Intel, más la integrada a la motherboard que tiene el equipo. El costo de cada una de las tarjetas que se pretende utilizar es de $800.00

## 4.7 Diseño

La colocación de los equipos OpenBSD en un piso determinado dependerá de la cantidad de equipos clientes que va a soportar y la distancia a la que se encuentren del mismo. Tomando en cuenta esa consideración, y viendo la cantidad de equipos distribuidos en cada departamento listado en la tabla anterior, se distribuyeron las ubicaciones donde estarán los equipos OpenBSD, como se muestra en la tabla 4.5.

| Ubicación de cada equipo OpenBSD | Departamento | Ubicación del departamento |
|---|---|---|
| Piso 7 | Desarrollo de Personal | Piso 9 |
| | Publicaciones | Piso 9 |
| | Catálogo Colectivo | Piso 9 |
| | Publicaciones periódicas | Piso 6 |
| Piso 7 | Fondo Antiguo | Piso 10 |
| | Aula de Capacitación | Piso 10 |
| | Tesis | Piso 8 |
| Piso 1 | Circulación Bibliográfica | Piso 1, 2, 3, 4 y 5 lado oriente |
| | Circulación Bibliográfica | Piso 1, 2, 3, 4 y 5 lado poniente |
| | Planeación | Planta Alta |
| Entrepiso | Secretaría Académica | Planta Alta |
| | Subdirección de Biblioteca Central | Planta Principal |
| | Circulación Bibliográfica | Planta Principal |
| | Consulta y Auto préstamo | Planta Principal |
| Entrepiso | Consulta | Entrepiso |
| Basamento | Técnico | Basamento |
| | Adquisiciones | Basamento |

Tabla 4.5 Distribución de las ubicaciones de los equipos con OpenBSD

Estamos requiriendo, de acuerdo con la distribución en la tabla, un mínimo de 17 segmentos de red privada, distribuidos en 6 equipos OpenBSD.

Estos equipos OpenBSD estarán a su vez apoyados, cada uno, por cierta cantidad de switches, que son los que tendrán la comunicación entre los equipos cliente y el equipo OpenBSD; la cantidad de switches dependerá de la cantidad de equipos que se conecten.

Los demás departamentos (Dirección, Subdirección Técnica, Subdirección de Informática, Producción y Sistemas) se quedan funcionando con IP's públicas, debido a la necesidad de utilizarlas por cuestiones de administración con los servidores.

Toda el área de la Unidad Administrativa y el departamento de Selección, Adquisición y Donación, ubicados en el nivel Basamento, están con IP's privadas, pero utilizando un firewall como medio de acceso a la red.

# CAPÍTULO 5

# IMPLEMENTACIÓN, PRUEBAS Y MANTENIMIENTO

## 5.1 Implementación de OpenBSD

El orden de cómo se colocó el equipo con operativo OpenBSD es el siguiente:

A las computadoras clientes se les asignó una IP privada del segmento 192.168.X.X; éstas tienen comunicación con un switch de marca 3Com o Extreme Networks, que recibe las peticiones y las manda al equipo OpenBSD en el que se aplican las políticas de acceso y la traducción de las direcciones de red a una IP 132.248.67.X válida. Ver la imagen 5.1.

Estos equipos OpenBSD se comunican de manera directa a un switch, y posteriormente al switch principal Alpine 3808; éste a su vez manda las peticiones de salida a través del Firewall Fortigate 3808, que es el último equipo para dar salida a los equipos a Internet.

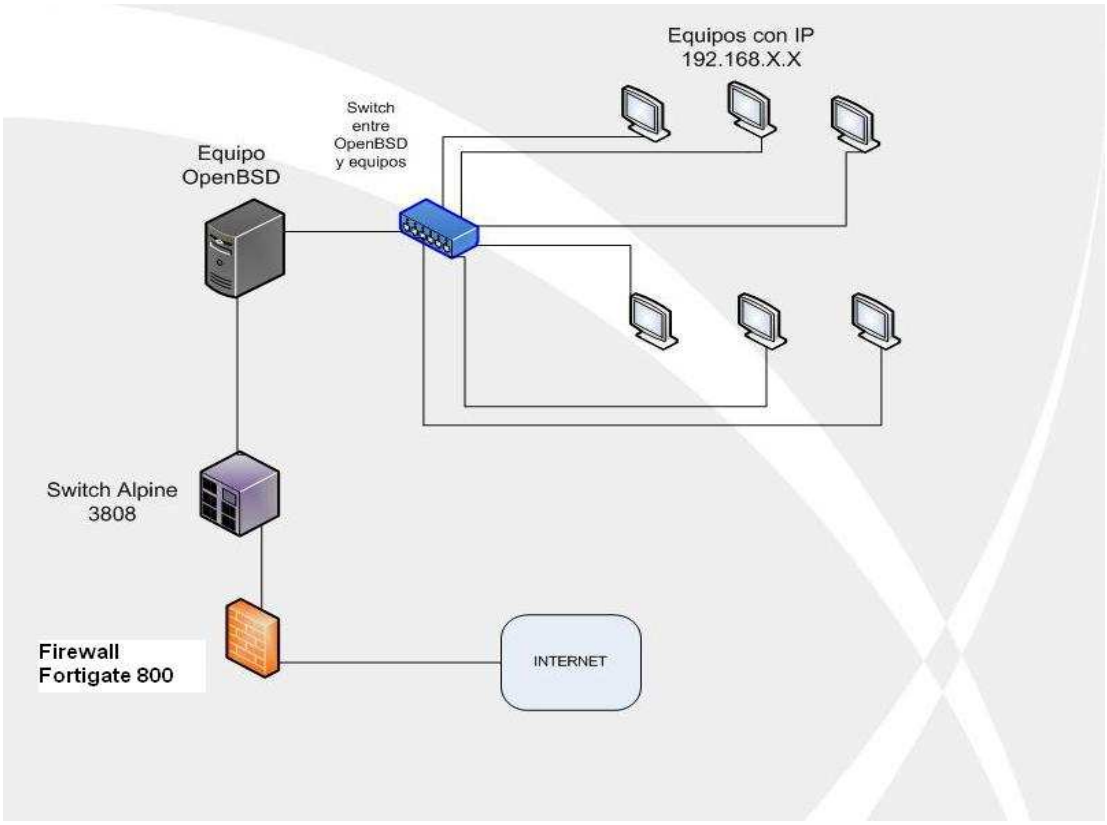



Imagen 5.1 Distribución de los equipos que interactúan con el OpenBSD

La estructura de los equipos OpenBSD colocados en las áreas definidas anteriormente es prácticamente la misma respecto a la imagen mostrada.

Si hay un equipo que busca un recurso que se encuentra disponible en su propia área, el OpenBSD se encarga de darle acceso sólo a los equipos de su área. Si el equipo está tratando de acceder a otro segmento, que no está permitido, el equipo OpenBSD no le da el servicio. En este punto, se evita el tráfico innecesario de peticiones a toda la red. Ver la imagen 5.2.

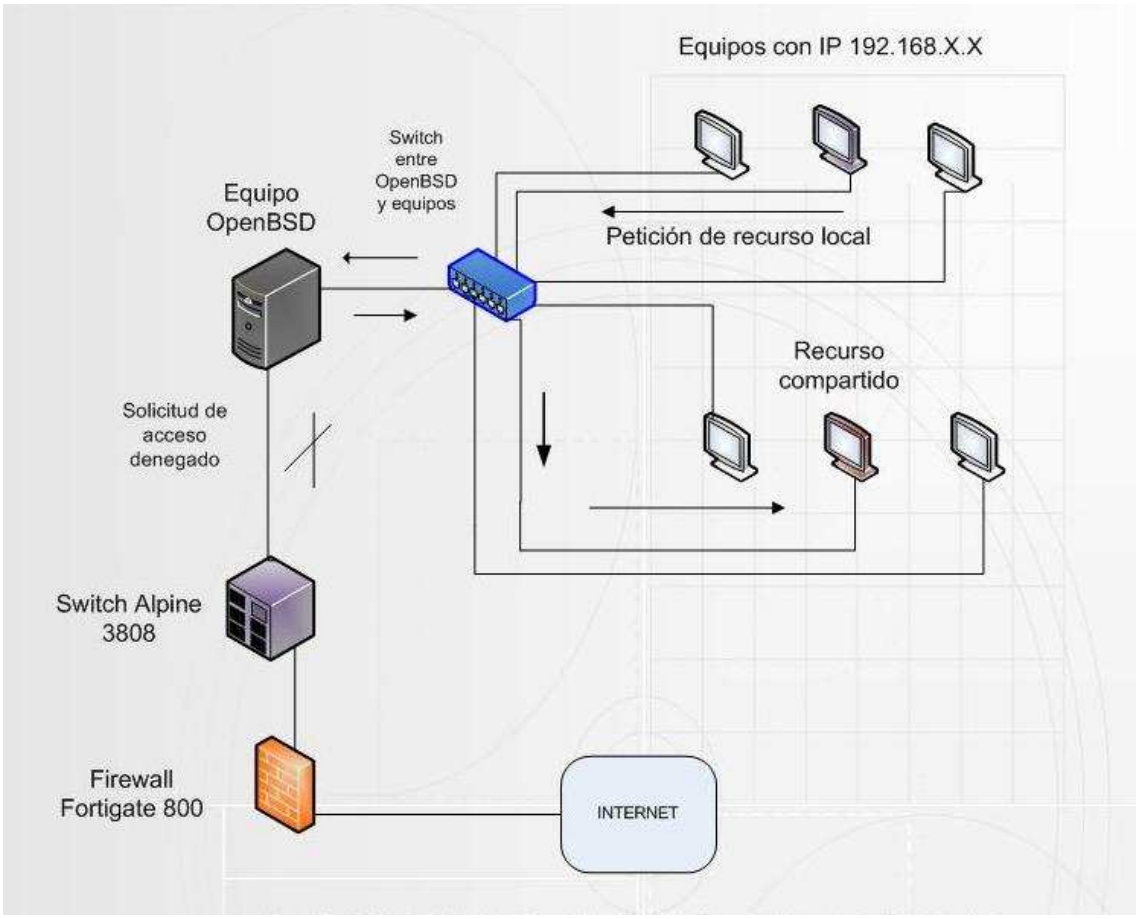



Imagen 5.2 Proceso de petición de servicios

La segmentación de la red se realizó por departamentos, aunque en algunos casos como el departamento de Circulación Bibliográfica, que tiene equipos en diferentes pisos de la Biblioteca Central, así como el departamento de Desarrollo de Personal, que se encuentra en dos niveles, se tuvieron que distribuir en 2 o más segmentos.

Se realizó la colocación de las tarjetas de red, definiendo en cada caso un segmento de red por cada tarjeta colocada en el equipo OpenBSD, en el cual por lo menos maneja tres, incluida la que el mismo equipo utiliza para dar salida a red.

## 5.2 Cambio de los segmentos de red

La tabla 5.1 muestra cómo se efectuó la segmentación de la red por departamento y por cantidad de equipos utilizados. En dicha tabla, se define el piso donde está ubicado el equipo, el departamento al cual da servicio, las IP's privadas que se utilizan, la IP pública con la que trabaja, la MAC address, la marca del equipo en el cual está montado el operativo, la serie, inventario y cantidad de tarjetas de red, disponibles y utilizadas.

El total de equipos que se utilizaron fueron 6, con un total de 17 segmentos.

Para poder dar acceso a esta distribución de direcciones privadas, se implementaron switches entre los equipos cliente y el OpenBSD, los cuales están distribuidos lo más cerca que se pudo de los equipos utilizados con el operativo OpenBSD. Un total de 22 switches, con su correspondiente cantidad de equipos que soportan, MAC y segmentos a los que dan servicio. Algunos de los switches se utilizaron como extensión o puente sin manejo de IP, debido a que no son administrables o no se requirió su control. No todos los switches se enlistan en la tabla, debido a que éstos dan servicio a las áreas excluidas de la segmentación. Ver tabla 5.2.

En la imagen 5.3, se muestran los equipos que se utilizaron para implementar el servicio por OpenBSD, y en la imagen 5.4, los switches colocados en el piso 8.

Imagen 5.3 Equipo Dell con operativo OpenBSD en Piso 7


Imagen 5.4 Switches en piso 8

| Piso | Servicio | Segmento | MAC | IP | E. Activo | Marca | Modelo | SubModelo | Serie | Inventario | Ptos. | Uso | Libre |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 7 | Puente Ext | 132.248.67.101 | 00:04:23:CB:72:70 | 132.248.67.101 | OpenBSD | Dell | Presicion 370 | WHM | FDCVZ61 | 2132658 | 5 | 5 | 0 |
| 7 | P. Periodicas | 192.168.16.X | 12:11:11 :A1:CA:E5 | 132.248.67.101 | OpenBSD | Dell | Presicion 370 | WHM | FDCVZ61 | 2132658 | 5 | 5 | 0 |
| 7 | Publicaciones | 192.168.19X | 00:04:23:CB:72:75 | 132.248.67.101 | OpenBSD | Dell | Presicion 370 | WHM | FDCVZ61 | 2132658 | 5 | 5 | 0 |
| 7 | Cat. Col. | 192.168.29.X | 00:04:23:CB:72:86 | 132.248.67.101 | OpenBSD | Dell | Presicion 370 | WHM | FDCVZ61 | 2132658 | 5 | 5 | 0 |
| 7 | Des. de Pers. | 192.168.39.X | 00:04:23:C7: 98:69 | 132.248.67.101 | OpenBSD | Dell | Presicion 370 | WHM | FDCVZ61 | 2132658 | 5 | 5 | 0 |
| 7 | Puente Ext | 132.248.67.181 | 00:11:11:B8:AF:8A | 132.248.67.181 | OpenBSD | Dell | Presicion 370 | WHM | 2K0GZ61 | 2132650 | 5 | 4 | 1 |
| 7 | Disponible | 192.168.32.X | 00:21:91:8C:FD:76 | 132.248.67.181 | OpenBSD | Dell | Presicion 370 | WHM | 2K0GZ61 | 2132650 | 5 | 4 | 1 |
| 7 | Fondo Antiguo | 192.168.21.X | 00:21:91:8D:17:09 | 132.248.67.181 | OpenBSD | Dell | Presicion 370 | WHM | 2K0GZ61 | 2132650 | 5 | 4 | 1 |
| 7 | Aula de Cap. | 192.168.20.X | 00:0E:0C:7F:7D:AE | 132.248.67.181 | OpenBSD | Dell | Presicion 370 | WHM | 2K0GZ61 | 2132650 | 5 | 4 | 1 |
| 7 | Disponib Tesis | 192.168.18.X | 00:0E:0C:7F:7A:40 | 132.248.67.181 | OpenBSD | Dell | Presicion 370 | WHM | 2K0GZ61 | 2132650 | 5 | 4 | 1 |
| Eco | Puente | 132.248.67.103 | 00:1B:21:1D:78:18 | 132.248.68.103 | OpenBSD | Dell | Presicion 370 | WHM | 5K0GZ61 | 2132649 | 3 | 3 | 0 |
| Eco | Consulta | 192.168.100.X | 00:04:23:C7:99:11 | 132.248.68.103 | OpenBSD | Dell | Presicion 370 | WHM | 5K0GZ61 | 2132649 | 3 | 3 | 0 |
| Eco | Consulta | 192.168.101.X | 00:04:23:C7:9A:C5 | 132.248.68.103 | OpenBSD | Dell | Presicion 370 | WHM | 5K0GZ61 | 2132649 | 3 | 3 | 0 |
| E | Puente | 132.248.67.95 | 00:13:20:07:50:10 | 132.248.67.95 | OpenBSD | Dell | Presicion 370 | WHM | 37BGH71 | 2190940 | 5 | 5 | 0 |
| E | Catálogo Elec. | 192.168.2.X | 00:21:91:8C:FD:6E | 132.248.67.95 | OpenBSD | Dell | Presicion 370 | WHM | 37BGH71 | 2190940 | 5 | 5 | 0 |
| E | Sec. Acad. | 192.168.5.X | 00:0E:0C:81:21:12 | 132.248.67.95 | OpenBSD | Dell | Presicion 370 | WHM | 37BGH71 | 2190940 | 5 | 5 | 0 |
| E | Catálogo Elec. | 192.168.3.X | 00:0E:0C:7F:7C:76 | 132.248.67.95 | OpenBSD | Dell | Presicion 370 | WHM | 37BGH71 | 2190940 | 5 | 5 | 0 |
| E | Sub. BC | 192.168.4.X | 00:0E:0C:7F:7D:20 | 132.248.67.95 | OpenBSD | Dell | Presicion 370 | WHM | 37BGH71 | 2190940 | 5 | 5 | 0 |
| 1 | Puente | 132.248.67.141 | 00:11:11:A1:BE:80 | 132.248.67.141 | OpenBSD | Dell | Presicion 370 | WHM | 5FCVZ61 | 2132659 | 5 | 5 | 0 |
| 1 | Planeacion | 192.168.11.X | 00:1B:21:1C:93:CC | 132.248.67.141 | OpenBSD | Dell | Presicion 370 | WHM | 5FCVZ61 | 2132659 | 5 | 5 | 0 |
| 1 | Pisos 5-3-2 | 192.168.12.X | 00:1B:21:1C:94:99 | 132.248.67.141 | OpenBSD | Dell | Presicion 370 | WHM | 5FCVZ61 | 2132659 | 5 | 5 | 0 |
| 1 | 1 y 4 Piso Pon. | 192.168.14.X | 00:1B:21:1C:93:55 | 132.248.67.141 | OpenBSD | Dell | Presicion 370 | WHM | 5FCVZ61 | 2132659 | 5 | 5 | 0 |
| 1 | 1 y 4 Piso Ori. | 192.168.15.X | 00:1B:21:1C:94:29 | 132.248.67.141 | OpenBSD | Dell | Presicion 370 | WHM | 5FCVZ61 | 2132659 | 5 | 5 | 0 |
| MDF | Puente | 132.248.67.62 | 00:11:11:BE:4E:EC | 132.248.67.62 | OpenBSD | Dell | Presicion 370 | WHM | 6DCVZ61 | 2132662 | 5 | 3 | 2 |
| MDF | Disponible | 192.168.23.X | 00:21:91:90:BC:49 | 132.248.67.62 | OpenBSD | Dell | Presicion 370 | WHM | 6DCVZ61 | 2132662 | 5 | 3 | 2 |
| MDF | Proc. Tecnicos | 192.168.24.X | 00:21:91:90:BC:56 | 132.248.67.62 | OpenBSD | Dell | Presicion 370 | WHM | 6DCVZ61 | 2132662 | 5 | 3 | 2 |
| MDF | Adquisiciones | 192.168.25.X | 00:21:91:90BC:5A | 132.248.67.62 | OpenBSD | Dell | Presicion 370 | WHM | 6DCVZ61 | 2132662 | 5 | 3 | 2 |
| MDF | Disponible | 192.168.26.X | 00:21:91:90:BB:94 | 132.248.67.62 | OpenBSD | Dell | Presicion 370 | WHM | 6DCVZ61 | 2132662 | 5 | 3 | 2 |

Tabla 5.1 Distribución de equipos OpenBSD en el edificio de la Biblioteca Central

| Piso | Servicio | Segmento | MAC | IP | E. Activo | Marca | Modelo | Serie | Inventario | Ptos. | Uso | Libre |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 10 | Fondo Antiguo | 192.168.21.X | 00:1C:C5:B9:A2:80 | Puente | Switch | 3Com | Superstack 3 4500 | YECF9JLB9A280 | 2271829 | 24 | 12 | 12 |
| 8 | Des. de Pers. | 192.168.39.X | 00:16:E0:87:66:40 | 132.248.67.197 | Switch | 3Com | Superstack 4200 | LDZV72H876640 | 2222570 | 48 | 17 | 31 |
| 8 | Tesis | 192.168.18.X | 00:16:E0:87:68:80 | 132.248.67.198 | Switch | 3Com | Superstack 4200 | LDZV72H876880 | 2222569 | 48 | 46 | 2 |
| 8 | Pub. Per. | 192.168.16.X | 00:16:E0:46:9A:40 | 132.248.67.209 | Switch | 3Com | Superstack 4250T | LY3V6HH469A40 | 2213528 | 48 | 25 | 23 |
| 8 | Aula de Cap. | 192.168.20.X | 00:12:A9:E4:25:E0 | 132.248.67.194 | Switch | 3Com | Superstack 4250T | LY3V5HDE425E0 | - | 48 | 27 | 21 |
| 8 | Cat. Col. | 192.168.29.X | 00:01:30:11:B2:EE | 132.248.67.244 | Switch | Extreme | SUMMIT 24E3 | 0315R-00249 | 2134375 | 24 | 16 | 8 |
| 8 | Publicaciones | 192.168.19.X | 00:01:30:11:B2:C3 | 132.248.67.196 | Switch | Extreme | SUMMIT 24E3 | 0315R-00206 | 2104879 | 24 | 12 | 12 |
| 1 | 1 y 4 Piso Pon. | 192.168.14.X | 00:1A:C1:0E:D3:C1 | 132.248.67.189 | Switch | 3Com | Superstack 4500 | YECF83K0ED3C0 | 2243225 | 24 | 14 | 10 |
| 1 | Planeacion | 192.168.11.X | 00:16:E0:46:5D:80 | 132.248.67.192 | Switch | 3Com | Superstack 4250T | LY3V6HH465D80 | 2213527 | 48 | 22 | 26 |
| 1 | 1 y 4 Piso Orien. | 192.168.15.X | 00:1A:C1:0E:EB:81 | 132.248.67.190 | Switch | 3Com | Superstack 4500 | YECF83K0EEB80 | 2243223 | 24 | 2 | 24 |
| 5 | Pisos 5-3-2 | Puente | No administrable | Puente | Switch | 3Com | Superstack 4250T | - | 1957361 | 24 | 7 | 17 |
| PP | Catálogo Elec. | 192.168.2.X | 00:22:57:32:F7:40 | Puente | Switch | 3Com | Superstack 3 4500 | YECFABN32F740 | 2271840 | 24 | 13 | 11 |
| PP | Catálogo Elec. | 192.168.3.X | 00:22:57:33:7D:80 | Puente | Switch | 3Com | Superstack 3 4500 | YECFABN337D80 | 2271839 | 24 | 19 | 2 |
| E | Sub. BC | 192.168.4.X | 00:1C:C5:B3:E4:40 | Puente | Switch | 3Com | Superstack 3 4500 | YECF9ELB3E440 | 2271830 | 24 | 16 | 8 |
| E | Sec. Acad. | 192.168.5.X | 00:1C:C5:39:E3:00 | Puente | Switch | 3Com | Superstack 3 4500 | YECF91L39E300 | 2247687 | 24 | 11 | 13 |
| ECo | Consulta | 192.168.100.X | 00:22:57:B9:FE:C0 | Puente | Switch | 3Com | Superstack 4500 | YEDFAWNB9FEC0 | 2288282 | 48 | 42 | 6 |
| ECo | Consulta | 192.168.101.X | 00:1E:C1:CE:CA:00 | Puente | Switch | 3Com | Superstack 4500 | YECF9WMCECA00 | - | 24 | 16 | 8 |
| 7 | Isabel Chong | Puente | No administrable | Puente | Switch | 3Com | Dual Speed 8 ptos | 7P1F095877 | 1777544 | 8 | 8 | 0 |
| PA | Rubén Bonifaz | Puente | No administrable | Puente | Switch | 3Com | Dual Speed 16 ptos | 7RFF094053 | 1968460 | 16 | 3 | 13 |
| MDF | Proc. Técnicos | 192.168.24.X | 00:04:96:05:56:4B | 132.248.67.245 | Switch | Extreme | Summit 200-48 | 0404G-01122 | 2181474 | 48 | 44 | 4 |
| MDF | Adquisiciones | 192.168.25.X | 00:04:96:05:54:C1 | 132.248.67.191 | Switch | Extreme | Summit 200-48 | 0404G-01120 | 2181472 | 48 | 24 | 24 |
| MDF | DGB | 132.248.67.X | 00:14:7C:10:57:20 | Puente | Switch | 3Com | Superstack 4250T | LY3V5ME105720 | 2132646 | 48 | 29 | 19 |
| MDF | DGB | 132.248.67.X | 00:24:73:38:EB:01 | 132.248.67.227 | Switch | 3Com | Superstack 3 4500 | YEDFBAP38EB00 | 2288279 | 48 | 13 | 35 |
| MDF | DGB | 132.248.67.X | 00:19:DB:BE:24:C4 | 132.248.67.24 | Firewall | Barracuda | Spam Firewall 300 | BAR-SF-101655 | 2247686 | 2 | 2 | 0 |
| MDF | DGB | 132.248.67.X | 00:09:0F:0C:A4:70 | 132.248.67.100 | Firewall | FORTINET | FORTIGATE 800 | FGT8003607501127 | 2249951 | 4 | 1 | 3 |
| MDF | DGB | 132.248.67.X | 00:04:96:00:6C:70 | 132.248.67.246 | Switch | ALPINE | 45080 | 03235-00498 | 2134371 | 8 | 5 | 3 |
| MDF | DGB | 132.248.67.X | 00:04:96:05:56:4C | 132.248.67.187 | Switch | Extreme | SUMMIT 200-48 | 0404G-01121 | 2181473 | 48 | 23 | 25 |
| Piso 9 | Edu Continua | Puente | No administrable | Puente | Switch | 3Com | Dual Speed 8 ptos | 7P1F268078 | 1968459 | 8 | 5 | 3 |

Tabla 5.2 Muestra la cantidad de switches utilizados para poder dar acceso a los equipos segmentados a la red

Una vez definidos los segmentos y la cantidad de equipos que estaban implicados en el proceso, se procedió a realizar la configuración de las tarjetas de red, los usuarios y las reglas de filtrado de paquetes para el correspondiente acceso a la red, vía OpenBSD.

Los archivos principales a utilizar son: por un lado, el sysctl.conf, que es el archivo de las configuraciones de las variables del kernel, el cual indica la implementación de IP forwarding en el equipo; por otro lado, el archivo pf.conf, que tiene las instrucciones para el control de paquetes TCP y UDP; y, por último, el archivo rc.conf, en el que se realiza la configuración a nivel de software.

De manera más descriptiva, se enlistan a continuación:

### 5.2.1 sysctl.conf

Con el archivo sysctl.conf se habilita el IP-forwarding o el reenvío de paquetes de una red a otra, para que cuando el equipo realice NAT se pueda completar el proceso de peticiones. En términos más generales, se habilita la funcionalidad de ruteo del servidor. Lo anterior se logra estableciendo la bandera de IP-forwarding a "1" en el archivo ubicado en /etc/sysctl.conf

Se tiene que reiniciar el equipo para que se habilite el reenvío de los paquetes. Se muestra la configuración del archivo en el equipo OpenBSD del área de procesos técnicos y adquisiciones.

```
$ more sysctl.conf
#       $OpenBSD: sysctl.conf,v 1.46 2008/01/05 18:38:37 mbalmer Exp $
#
# This file contains a list of sysctl options the user wants set at
# boot time. See sysctl(3) and sysctl(8) for more information on
# the many available variables.
#
net.inet.ip.forwarding=1        # 1=Permit forwarding (routing) of IPv4 packets
#net.inet.ip.mforwarding=1      # 1=Permit forwarding (routing) of IPv4 multicast packets
#net.inet.ip.multipath=1        # 1=Enable IP multipath routing
#net.inet6.ip6.forwarding=1     # 1=Permit forwarding (routing) of IPv6 packets
#net.inet6.ip6.mforwarding=1    # 1=Permit forwarding (routing) of IPv6 multicast packets
#net.inet6.ip6.multipath=1      # 1=Enable IPv6 multipath routing
#net.inet6.ip6.accept_rtadv=1   # 1=Permit IPv6 autoconf (forwarding must be 0)
#net.inet.tcp.rfc1323=0         # 0=Disable TCP RFC1323 extensions (for if tcp is slow)
#net.inet.tcp.rfc3390=0         # 0=Disable RFC3390 for TCP window increasing
#net.inet.esp.enable=0          # 0=Disable the ESP IPsec protocol
#net.inet.ah.enable=0           # 0=Disable the AH IPsec protocol
#net.inet.esp.udpencap=0        # 0=Disable ESP-in-UDP encapsulation
#net.inet.ipcomp.enable=1       # 1=Enable the IPCOMP protocol
#net.inet.etherip.allow=1       # 1=Enable the Ethernet-over-IP protocol
#net.inet.tcp.ecn=1             # 1=Enable the TCP ECN extension
#net.inet.carp.preempt=1        # 1=Enable carp(4) preemption
#net.inet.carp.log=1            # 1=Enable logging of carp(4) packets
#ddb.panic=0                    # 0=Do not drop into ddb on a kernel panic
```

```
#ddb.console=1                  # 1=Permit entry of ddb from the console
#fs.posix.setuid=0              # 0=Traditional BSD chown() semantics
#vm.swapencrypt.enable=0        # 0=Do not encrypt pages that go to swap
#vfs.nfs.iothreads=4            # Number of nfsio kernel threads
#net.inet.ip.mtudisc=0          # 0=Disable tcp mtu discovery
#kern.usercrypto=0              # 0=Disable userland use of /dev/crypto
#kern.splassert=2               # 2=Enable with verbose error messages
#kern.nosuidcoredump=2          # 2=Put suid coredumps in /var/crash
#kern.watchdog.period=32        # >0=Enable hardware watchdog(4) timer if available
#kern.watchdog.auto=0           # 0=Disable automatic watchdog(4) retriggering
#machdep.allowaperture=2        # See xf86(4)
#machdep.apmwarn=10             # battery % when apm status messages enabled
#machdep.apmhalt=1              # 1=powerdown hack, try if halt -p doesn't work
#machdep.kbdreset=1             # permit console CTRL-ALT-DEL to do a nice halt
#machdep.userldt=1              # allow userland programs to play with ldt,
                                # required by some ports
#kern.emul.aout=1               # enable running dynamic OpenBSD a.out bins
#kern.emul.bsdos=1              # enable running BSD/OS binaries
#kern.emul.freebsd=1            # enable running FreeBSD binaries
#kern.emul.ibcs2=1              # enable running iBCS2 binaries
#kern.emul.linux=1              # enable running Linux binaries
#kern.emul.svr4=1               # enable running SVR4 binaries
```

En las primeras líneas se observa cómo se habilita el IP-forwarding y deshabilitan los demás servicios que no necesitamos.

Conforme se libere una nueva versión del operativo, se irá actualizando el equipo. Hasta el momento se ha actualizado en promedio 1 vez al año. Esta configuración es la misma para todos los servidores OpenBSD instalados.

### 5.2.2 rc.conf

En el archivo pf.conf se configuran los servicios del sistema que uno quiere que se habiliten. En este caso, como se tiene que habilitar el Packet Filter, que es el sistema de filtrado de tráfico TCP/IP propia de las distribuciones OpenBSD, se edita el archivo ubicado en /etc/rc.conf y se cambia la línea que indica el Packet Filter a “YES”; para que los cambios surtan efecto, se necesita reiniciar el sistema. Al reiniciar, tendremos habilitado el equipo para el filtrado de paquetes en IPv4.

```
# more rc.conf
#!/bin/sh -
#
#       $OpenBSD: rc.conf,v 1.130 2008/06/09 22:21:49 mbalmer Exp $

# set these to "NO" to turn them off.  otherwise, they're used as flags
ripd_flags=NO           # for normal use: ""
mrouted_flags=NO        # for normal use: "", if activated
                        # be sure to enable multicast_router below.
dvmrpd_flags=NO         # for normal use: ""
ospfd_flags=NO          # for normal use: ""
ospf6d_flags=NO         # for normal use: ""
```

```
bgpd_flags=NO          # for normal use: ""
rarpd_flags=NO         # for normal use: "-a"
bootparamd_flags=NO    # for normal use: ""
rbootd_flags=NO        # for normal use: ""
sshd_flags=""          # for normal use: ""
named_flags=NO         # for normal use: ""
rdate_flags=NO         # for normal use: [RFC868-host] or [-n RFC2030-host]
timed_flags=NO         # for normal use: ""
ldattach_flags=NO      # for normal use: "[options] linedisc cua-device"
ntpd_flags=NO          # for normal use: ""
isakmpd_flags=NO       # for normal use: ""
sasyncd_flags=NO       # for normal use: ""
mopd_flags=NO          # for normal use: "-a"
apmd_flags=NO          # for normal use: ""
dhcpd_flags=NO         # for normal use: ""
dhcrelay_flags=NO      # for normal use: "-i interface [server]"
rtadvd_flags=NO        # for normal use: list of interfaces
                # be sure to set net.inet6.ip6.forwarding=1
route6d_flags=NO       # for normal use: ""
                # be sure to set net.inet6.ip6.forwarding=1
rtsold_flags=NO        # for normal use: interface
                # be sure to set net.inet6.ip6.forwarding=0
                # be sure to set net.inet6.ip6.accept_rtadv=1
lpd_flags=NO           # for normal use: "" (or "-l" for debugging)
sensorsd_flags=NO      # for normal use: ""
hotplugd_flags=NO      # for normal use: ""
watchdogd_flags=NO     # for normal use: ""
ftpproxy_flags=NO      # for normal use: ""
hostapd_flags=NO       # for normal use: ""
ifstated_flags=NO      # for normal use: ""
relayd_flags=NO        # for normal use: ""
snmpd_flags=NO         # for normal use: ""

# use -u to disable chroot, see httpd(8)
httpd_flags=NO         # for normal use: "" (or "-DSSL" after reading ssl(8))

# For normal use: "-L sm-mta -bd -q30m", and note there is a cron job
sendmail_flags="-L sm-mta -C/etc/mail/localhost.cf -bd -q30m"
spamd_flags=NO         # for normal use: "" and see spamd(8)
spamd_black=NO         # set to YES to run spamd without greylisting
spamlogd_flags=""      # use eg. "-i interface" and see spamlogd(8)

# Set to NO if ftpd is running out of inetd
ftpd_flags=NO          # for non-inetd use: "-D"

# Set to NO if identd is running out of inetd
identd_flags=NO        # for non-inetd use: "-b -elo"

# On some architectures, you must also disable console getty in /etc/ttys
xdm_flags=NO           # for normal use: ""

# For enabling console mouse support (i386 alpha amd64)
wsmoused_flags=NO      # for ps/2 or usb mice: "", serial: "-p /dev/cua00"

# set the following to "YES" to turn them on
rwhod=NO
```

```
nfs_server=NO          # see sysctl.conf for nfs client configuration
lockd=NO
amd=NO
pf=YES                 # Packet filter / NAT
ipsec=NO               # IPsec
portmap=NO             # Note: inetd(8) rpc services need portmap too
inetd=NO               # almost always needed
check_quotas=YES       # NO may be desirable in some YP environments
accounting=NO          # process accounting (using /var/account/acct)

krb5_master_kdc=NO     # KerberosV master KDC. Run 'info heimdal' for help.
krb5_slave_kdc=NO      # KerberosV slave KDC.
afs=NO                 # mount and run afs

# Multicast routing configuration
# Please look at netstart(8) for a detailed description if you change these
multicast_host=NO      # Route all multicast packets to a single interface
multicast_router=NO    # A multicast routing daemon will be run, e.g. mrouted

# miscellaneous other flags
# only used if the appropriate server is marked YES above
savecore_flags=                # "-z" to compress
ypserv_flags=                  # E.g. -1 for YP v1, -d for DNS etc
yppasswdd_flags=NO             # "-d /etc/yp" if passwd files are in /etc/yp
nfsd_flags="-tun 4"            # Crank the 4 for a busy NFS fileserver
amd_dir=/tmp_mnt               # AMD's mount directory
amd_master=/etc/amd/master     # AMD 'master' map
syslogd_flags=                 # add more flags, ie. "-u -a /chroot/dev/log"
pf_rules=/etc/pf.conf          # Packet filter rules file
ipsec_rules=/etc/ipsec.conf    # IPsec rules file
pflogd_flags=                  # add more flags, ie. "-s 256"
afsd_flags=                    # Flags passed to afsd
shlib_dirs=                    # extra directories for ldconfig, separated
                               # by space

local_rcconf="/etc/rc.conf.local"

[ -f ${local_rcconf} ] && . ${local_rcconf} # Do not edit this line
```

### 5.2.3 pf.conf

El archivo pf.conf se ubica en /etc/pf.conf. Este archivo está dividido en 7 partes.

- **Macros**: Variables definidas por el usuario, por ejemplo: direcciones IP, nombre de interfaces, etc.
- Tablas: Estructura que contiene listas de direcciones IP
- Opciones: Opciones que controlan el comportamiento de pf.
- Scrubs: Reprocesamiento de paquetes para normalizarlos o desfragmentarlos
- Colas: Control de ancho de banda y priorización de paquetes
- **Traducción**: NAT y dirección de paquetes
- **Reglas de filtrado**: Controla el filtrado de paquetes

A excepción de los macros y las tablas, cada una de las secciones que les siguen debe de aparecer en estricto orden dentro del archivo de configuración. No es necesario que aparezcan todas las secciones.

Una lista permite especificación múltiple de reglas con criterios similares. Ejemplo:

*block out on bge0_if from 224.0.0.1 to any*
*block in on bge0_if proto {tcp,udp} from any to 132.248.67.255 port 137*

Estas listas pueden ser direcciones IP, de puertos o servicios, pueden incluirse varias de ellas en cada regla y pueden ser anidadas. Las macros son variables definidas por el usuario, cuyo fin es simplificar el mantenimiento del archivo y reducir la complejidad del mismo. Para hacer uso de la macro, se hace referencia con el signo de $, de esta manera se sustituirá por su valor al ser leído.

*ext_if="bge0"*
*block out on $ext_if from 224.0.0.1 to any*

Se muestra el archivo pf.conf utilizado para el departamento de Procesos Técnicos y Adquisiciones.

```
$ more pf.conf
pf.conf: Permission denied
$ su
Password:
# more pf.conf
#       $OpenBSD: pf.conf,v 1.37 2008/05/09 06:04:08 reyk Exp $
#
# See pf.conf(5) for syntax and examples.
# Remember to set net.inet.ip.forwarding=1 and/or net.inet6.ip6.forwarding=1
# in /etc/sysctl.conf if packets are to be forwarded between interfaces.

ext_if="bge0"                                          Definiendo las macros
int1_if="sk0"   # Rango
int2_if="sk1"   # Rango del Técnico  192.168.24.0/24
int3_if="sk2"   # Rango de Adquisiciones  192.168.25.0/24
int4_if="sk3"   # Rango
internal1="192.168.23.0/24"
internal2="192.168.24.0/24"
internal3="192.168.25.0/24"
internal4="192.168.26.0/24"
external="132.248.67.62"

#nat on $ext_if from $internal1 to any -> ($ext_if)
nat on $ext_if from $internal2 to any -> ($ext_if)     Definiendo el NAT
nat on $ext_if from $internal3 to any -> ($ext_if)
#nat on $ext_if from $internal4 to any -> ($ext_if)
pass all
antispoof quick for bge0 inet
block in on $ext_if proto { igmp } from any to 132.248.67.62    Definiendo las reglas de filtrado
block out on $ext_if proto { igmp } from any to 132.248.67.62
```

```
block out on $ext_if from 224.0.0.1 to any
block return in  quick on $ext_if from any to 224.0.0.1
block in  on $ext_if from any to 0.0.0.0
block in  on $ext_if proto {tcp,udp} from any to 132.248.67.255 port 137
block in  on $ext_if proto {tcp,udp} from any to 132.248.67.255 port 138
block in  on $ext_if proto {tcp,udp} from any to 132.248.67.255 port 17500

block in  on $ext_if from any to 255.255.255.255
block in  on $int2_if from any to 255.255.255.255
block in  on $int3_if from any to 255.255.255.255
block out on $ext_if from any to 0.0.0.0
```

La configuración de los equipos OpenBSD, a excepción del que se ubica en el área de Consulta, tienen prácticamente la misma configuración; el equipo ubicado en el departamento de Consulta requirió más líneas de instrucción debido a las necesidades y peticiones del departamento, dado que ofrecen servicios de bases de datos, red y tesis de manera separada. Ver Anexo.

En lo referente a los permisos para el uso de red, se le dio la carga al firewall de la biblioteca.

## 5.3 Pruebas

Se realizaron pruebas de acceso local y externo a las áreas trabajadas, como los archivos compartidos, acceso a las impresoras en red, salida a Internet y el acceso a los servicios de bases de datos Alephv16. En la mayor parte de los casos, la comunicación fue transparente, a excepción de la comunicación de los clientes de Alephv16 con los servidores, debido a que se necesitaba habilitar la nueva IP de cada área para ingresar, porque se tiene control de acceso, vía firewall. Lo mismo pasó con las impresoras en red: se les cambió la IP de destino tanto en la impresora como en la PC.

El servicio de antivirus corporativo en un principio no dejaba actualizar, pero conforme se dieron los permisos necesarios funcionó correctamente; lo mismo pasó con el servidor de actualizaciones Windows, se realizó la correspondiente actualización y funcionó de manera normal.

Se realizaron pruebas de rendimiento encendiendo todos los equipos al mismo tiempo, realizando actualizaciones y algunas peticiones a red, las cuales no redujeron la velocidad de comunicación en los servicios.

Estas redes segmentadas, a excepción de la que opera en el departamento de consulta, permiten un acceso transparente a los sistemas de bases de datos referenciales que tiene a su disposición la Biblioteca Central, como son LIBRUNAM, SERIUNAM, TESIUNAM, MAPAMEX, etc.

Así mismo, permite: Acceso a Internet, Acceso a correo electrónico institucional, Acceso a Tesis digitales, Acceso a libros y revistas digitales.

En general, esta organización de redes segmentadas opera de manera tal que los usuarios finales no notan la diferencia entre tener la IP privada y la IP pública que tenían, salvo lo que se definió en las reglas del firewall, políticas que están fuera de este proyecto.

Se hicieron también pruebas de acceso para los usuarios administradores mediante Secure Shell; sólo el departamento de Producción puede realizar las modificaciones pertinentes en estos servidores OpenBSD.

Algo importante que se realizó durante las fases de cambio de IP fue la realización de sólo un área a la vez, por cualquier eventualidad que se presentara, lo cual sí ocurrió, pero de manera mínima.

## 5.4 Mantenimiento

Para el mantenimiento de estos equipos, se tiene un plan con lo siguiente:

- Limpieza física durante los periodos vacacionales, por lo menos 2 veces al año.
- Actualización o reinstalación del operativo OpenBSD por lo menos 1 vez al año, o hasta que salga una nueva versión de este operativo.
- Cambiar los switches que no son administrables por los que si son administrables conforme el presupuesto lo permita.
- Adquisición de insumos o refacciones que necesita este sistema de red: fuentes de poder, tarjetas de red, cables UTP, discos duros, memoria etc.
- Mantener un stock de computadoras del modelo utilizado, para cualquier eventualidad que hubiera.

Debido a que estos insumos, salvo las fuentes de poder y las tarjetas de red, se tienen en cantidades suficientes, el costo del mantenimiento es mínimo, comparado con lo que se obtuvo como resultado.

## 5.5 Control de inventario de los equipos en red

Es importante tener un buen control de los equipos, tanto del equipo activo como del equipo final, que es el de los usuarios. Para eso, se diseñó en su momento, por parte del departamento de Sistemas, una base con la relación de equipos por inventario y su ubicación que ayuda a ubicar algún equipo que se encuentre fallando y que sólo se puede detectar por MAC o IP.

El control de inventarios se hace evidente cuando se realiza el censo, como el que se hace anualmente en la UNAM. A parte de que es una práctica sana, se tiene mejor control de los bienes y se puede dar una mejor idea de lo que disponemos y qué está funcionando actualmente, para poder realizar una toma de decisión respecto a renovaciones de equipo. Se muestra la página de control de inventarios que utiliza para control interno la DGB en la imagen 5.5.

Una lista concreta respecto al equipo utilizado en este proyecto se mostró en las tablas anteriores, indicando los equipos OpenBSD y switches utilizados.

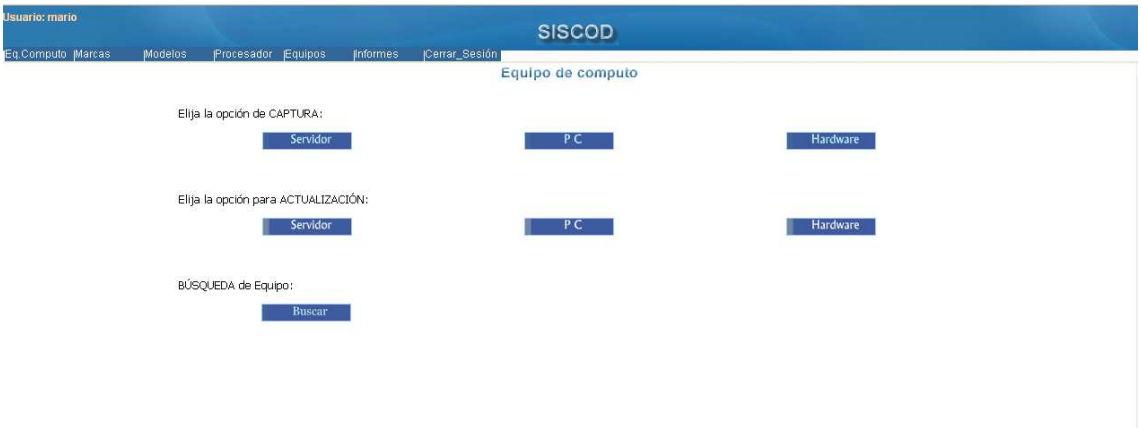



Imagen 5.5 Página para el control de inventarios de la Biblioteca Central

# CONCLUSIONES

El edificio de la Biblioteca Central de la Universidad Nacional Autónoma de México, catalogada como Patrimonio Mundial de la Humanidad, tiene que encontrarse a la vanguardia respecto a los servicios que proporciona. Ante esta situación, el tener y mantener la infraestructura de telecomunicaciones al día es imprescindible para el correcto funcionamiento de estos servicios.

El constante cambio de la tecnología y el uso de la información en la Biblioteca Central determinó que se implementaran nuevos servicios y como consecuencia surgieron otras necesidades, como la de incrementar la cantidad de nodos y poder darles acceso a la red, tanto interna como externa.

**Esto originó el problema de falta de IP's públicas y DHCP insuficiente, debido a la demanda de servicios ofrecidos.**

Ante la situación en que se encontraba la red de la Biblioteca Central respecto a la limitante de direcciones IP, para poder abastecer los servicios de red en la totalidad de equipos, y con base en los crecientes servicios que se han implementado, se tuvo la necesidad de dar solución a la falta de direcciones IP mediante algún método, técnica o procedimiento para resolver el problema.

En el capítulo 2, se recopiló información teórica respecto al ambiente de redes en el que la Biblioteca Central se desenvuelve, como el tipo de topología, tipo de red, los elementos de red con los que interactúan los equipos, y los protocolos que debemos conocer para la correcta comunicación en ese ambiente, que son los aplicados al modelo OSI y TCP/IP. Se revisó cómo funciona el direccionamiento IP y la clase a la que corresponde la UNAM.

Se realizó una compilación de información del equipo activo, como el switch, router y firewall, con el que se podía realizar el proceso de la segmentación o apoyarlo. Se revisó también el medio de transmisión por el que la información pasa de manera alámbrica y el concepto de cableado estructurado. Se visualizó y se mostró lo que la Biblioteca Central tiene respecto a estos dispositivos e infraestructura de cableado estructurado de manera real.

La cantidad de switches, routers y firewall disponibles en el mercado, más aparte la manera en cómo trabajan para dar paso a la información, es muy variada. Los switches 3Com y Extreme Networks, son los que se utilizaron en la red de la BC.

Dentro de la fase de análisis y diseño de este proyecto, se verificó la disponibilidad de los recursos que se necesitan, como la infraestructura de cableado estructurado que con anterioridad, y dada la envergadura del proyecto, un equipo de trabajo intervino para su realización. A su vez, los dispositivos que son

necesarios para la red LAN y las computadoras requeridas ya se encontraban disponibles, además del equipo, que ya estaba activo.

Se realizó una evaluación de la ubicación de los equipos de los usuarios, en cantidades y necesidades en cada departamento de la BC. El equipo que se decidió utilizar para la implementación de este servicio de IP's privadas fue un equipo Workstation Precision 370, dada la cantidad de puertos PCI que podían ser configurados para el uso de tarjetas de red, disponiendo de un total de 5 puertos de red.

El software a tomar se decidió que fuera el sistema operativo OpenBSD, dado que es un sistema operativo libre multiplataforma orientado a la portabilidad, estandarización, seguridad y criptografía. El software es de carácter gratuito y sus requerimientos de hardware son mínimos.

Considerando los puntos anteriores, se empezó a realizar la implementación del servicio dado que cumplía con las expectativas de lo que se había planteado el Departamento de Producción, y con la información recopilada se determinó colocar siete equipos en los niveles 7, 1, entrepiso y basamento. Se estableció la cantidad de nodos de que podía disponer cada departamento y el segmento de red privada que le correspondía.

Ya definido este punto, se procedió a la instalación y configuración de los servidores OpenBSD mediante el filtrado de paquetes y la traducción de direcciones de red, y al final el cambio de las direcciones de red en cada equipo.

Se realizaron pruebas de acceso local y externo a las áreas trabajadas. En la mayor parte de los casos, la comunicación fue transparente, a excepción de la comunicación de los clientes de Alephv16 con los servidores, debido a que se necesitaba habilitar la nueva IP de cada área para ingresar, porque se tiene control de acceso vía firewall. Lo mismo pasó con las impresoras en red: se les cambió la IP de destino tanto en la impresora como en la PC.

Como precaución, se realizó el cambio de IP de manera escalonada, cambiando las IP's de un solo departamento a la vez. Se realizaron pruebas de rendimiento encendiendo todos los equipos al mismo tiempo, realizando actualizaciones y algunas peticiones a red, las cuales no redujeron la velocidad de comunicación en los servicios.

Al tener realizado el proceso de pruebas y accesos, se procedió a realizar la documentación para tener control del equipo utilizado.

La elección de esta manera de operar se basó en las ventajas que nos proporcionaba, debido a que ya se disponía prácticamente de toda la infraestructura de cómputo y de red, así como el conocimiento del sistema operativo a utilizar, el cual sólo requirió de una revisión de los procedimientos y archivos dentro del sistema operativo que hacen que funcione la traducción de

direcciones y el filtrado de paquetes. Para el cambio de IP, colocación de switches y preparación de equipos, se realizó con el apoyo del equipo de trabajo del Departamento de Producción, debido a la gran cantidad de equipo que se tenía que mover, configurar y revisar.

Lo que se obtuvo con la segmentación de la red fue lo siguiente:

- Con una sola IP pública se da servicio a determinada cantidad de equipos por departamento
- Se liberan IP's públicas para futuros usos
- Se reducen peticiones de red innecesarias, las peticiones locales se quedan en su propio segmento, reduciendo el consumo de ancho de banda
- Mejor control del equipo de cómputo, mediante el registro de los datos de red y ubicación
- Se da servicio de red a la totalidad de equipos en el edificio de la BC

Con la correspondiente evaluación del desempeño de la red, se observó que no se requiere de equipo sofisticado para poder realizar este tipo de configuración en un área de trabajo; una computadora, el operativo y un switch de cualquier marca, si es que se necesitara, es el requerimiento mínimo, además de que el cambio de IP fue transparente para el usuario, y se pudieron liberar IP's públicas. De todas las IP's públicas que tenemos a disposición, se tienen tan sólo 102 ocupadas.

Esta forma de trabajar segmentando la red ya se tiene trabajando desde 2009, y no se han tenido más que pequeños problemas relacionados con los servicios ya establecidos, o cuando el usuario se mueve de lugar o departamento, entonces se cambia la IP que tenía a la que le corresponde en su nuevo lugar.

La forma como se está manejando el acceso a la red puede también tener fallas en el rendimiento del hardware, dado que, debido al uso, tiende a degradarse por las mismas características del hardware o del software.

Los equipos y los sistemas operativos tienden a evolucionar conforme pasa el tiempo, lo mismo pasa con las técnicas de administración de redes y las mejoras en los protocolos de red.

Conforme va llegando nueva tecnología y nuevos sistemas operativos con ventajas sumamente considerables a lo que se tiene con el OpenBSD y el modelo de PC usado, será necesario tomar nuevas medidas respecto a lo que resulte mejor para operar estos segmentos de red, o en su caso cambiar parcial o totalmente el método.

El sistema operativo OpenBSD es un sistema seguro si se configura correctamente; cada medio año libera una nueva versión con nuevas modificaciones o correcciones. Se seguirá utilizando el operativo, salvo que se encuentre otra opción mejor de software. Lo mismo pasará con el hardware: si se

encuentra una mejor opción y si está al alcance, se tomará o por lo menos se evaluará.

No queda más que dar las gracias a todo el Departamento de Producción al cual pertenezco y que, como equipo de trabajo, realizamos proyectos de esta envergadura.

# ANEXO

## Configuración del archivo pf.conf en el área de consulta

```
#	$OpenBSD: pf.conf,v 1.37 2008/05/09 06:04:08 reyk Exp $
#
# See pf.conf(5) for syntax and examples.
# Remember to set net.inet.ip.forwarding=1 and/or net.inet6.ip6.forwarding=1
# in /etc/sysctl.conf if packets are to be forwarded between interfaces.

#ext_if="ext0"
#int_if="int0"

#A continuación se definen las MACROS a usar para definir la red:

ext_if="em2"    # Definición del acceso a la RedDGB conocida como em2
int1_if="em0"    # Definición del acceso a la Red interna 1 segmento 100 conocida como em0
int2_if="em1"    # Definición del acceso a la Red interna 2 segmento 101 conocida como em1

red_dgb="132.248.67.0/24"
internal1="198.162.100.0/24"
internal2="198.162.101.0/24"
cyberadmin_server="192.168.100.51"
ip_validator="132.248.67.109"
ip_wsus="132.248.67.27"

#Líneas que definen las configuraciones de TESIS DIGITALES
#Configuraciones para la 132.248.9.25

www_aleph8991fenix="132.248.9.9"
www_oreon="132.248.67.65"

#A continuación se definen las MACROS a usar para definir los servicios de la LAN hacia
#la RedDGB y a la RedUNAM, para garantizar la política que nos norma para el uso
#de los recursos de Red asignados por la DGSCA "Políticas de Uso Aceptable de RedUNAM":

#Macros que limitarán el servicio NO AUTORIZADOS

www_bc="132.248.67.11"
www_bidi="132.248.9.9"
www_dgb="132.248.67.111"
www_ahau="132.248.9.25"
# Definición para el acceso a este equipo
web_serv_int = "192.168.100.52"
web_serv_ext = "132.248.67.103"
```

```
#La IP 192.168.100.254 está reservada para gateway de este equipo.
#La IP 192.168.101.254 está reservada para gateway de este equipo.


#Esta tabla define el trabajo de las nueve PCS de tesis digitales
table <tesdigi> { 192.168.101.2, 192.168.101.3, 192.168.101.4, 192.168.101.5,
192.168.101.6, 192.168.101.7,\
192.168.101.8, 192.168.101.9 }

#Esta tabla define el trabajo de las tres PCS de consulta de bases de datos
table <basescds> { 192.168.100.10, 192.168.100.11, 192.168.100.12 }

#Esta tabla define el trabajo de las veintiocho PCS con acceso a Internet por CyberAdmin
Server (192.168.100.51)
table <internet> { 192.168.100.13, 192.168.100.14, 192.168.100.15, 192.168.100.16,
192.168.100.17, 192.168.100.18, \
192.168.100.19, 192.168.100.20, 192.168.100.21, 192.168.100.22, 192.168.100.23,
192.168.100.24, 192.168.100.25,\
192.168.100.26, 192.168.100.27, 192.168.100.28, 192.168.100.29, 192.168.100.30,
192.168.100.31, 192.168.100.39, \
192.168.100.40, 192.168.100.41, 192.168.100.42, 192.168.100.43, 192.168.100.44,
192.168.100.45, 192.168.100.46, \
192.168.100.47, 192.168.100.51 }

#Esta tabla define el trabajo de las tres PCS de sólo impresión
table <impofice> { 192.168.100.36, 192.168.100.37, 192.168.100.38 }

#Esta tabla define el trabajo de PC de sólo consulta catálogo TESIUNAM
table <catalogo> { 192.168.100.35 }

#Esta tabla define la Primera Impresora (sólo impresión)
table <solo_printer> { 192.168.100.49 }

#Esta tabla define la Segunda Impresora (Internet y Bases de datos)
table <cyberadmin_printer> { 192.168.100.56 }

#Esta tabla define la Tercera Impresora (Tesis Digitales)
table <tesis_printer> { 192.168.101.48 }

#Esta tabla define la PC de la Jefatura de Consulta, Técnicos Académicos y secretaria.
table <academicos> { 192.168.101.52, 192.168.101.53, 192.168.101.54, 192.168.101.51,
192.168.101.68, 192.168.101.70, 192.168.101.60 }

#table <spamd-white> persist

#set skip on lo

scrub in

#nat-anchor "ftp-proxy/*"
```

```
#rdr-anchor "ftp-proxy/*"
#rdr-anchor "relayd/*"
nat on $ext_if from $int1_if/24 -> $ext_if
nat on $ext_if from $int2_if/24 -> $ext_if

#rdr  on $ext_if proto tcp from 132.248.67.0/24 to any port 80 -> 192.168.100.52
rdr  on $ext_if proto tcp from 132.248.67.0/24 to any port 80 -> 192.168.101.52

#binat on $ext_if from  $web_serv_int to any  -> $web_serv_ext

pass in all
block out on $int1_if proto { udp tcp } from any to any port 25
block out on $int1_if proto { udp tcp } from any to any port 110
block in on $int1_if proto { udp tcp } from <internet> to $www_oreon port 8991
block in on $int1_if proto { udp tcp } from <internet> to 132.248.67.11
block in on $int1_if proto { udp tcp } from <internet> to 132.248.67.111
block in on $int1_if proto { udp tcp } from <internet> to 132.248.9.9
block in on $int1_if proto { udp tcp } from <internet> to 132.248.9.25
block in on $int1_if proto { udp tcp } from <catalogo> to 132.248.9.9
block in on $int1_if proto { udp tcp } from <catalogo> to 132.248.9.25
# Agregado por Marcial 23 Junio 2010 b1
block in  quick on $ext_if proto { tcp,udp } from any to 132.248.67.255 port 137
block in  quick on $ext_if proto { tcp,udp } from any to 132.248.67.255 port 138
block in  quick on $ext_if proto { tcp,udp } from any to 132.248.67.255 port 17500

block in  quick on $ext_if from any to 255.255.255.255
block in  quick on $int1_if from any to 255.255.255.255
block in  quick on $int2_if from any to 255.255.255.255
# fin b1
pass out log quick on $int1_if proto { udp tcp } from 192.168.100.51 to any port 80

block out log on $int1_if proto { udp tcp } from 192.168.100.51 to any
pass out on $ext_if from $int1_if to any
pass out on $ext_if from $int2_if to any
```

# GLOSARIO

| | |
|---|---|
| ALGOL | Algorithmic Language |
| ARP | Address Resolution Protocol |
| ATM | Asynchronous Transfer Mode |
| BC | Biblioteca Central |
| BX | Bidirectional single fiber |
| CATV | Community Antenna Television |
| CRC | Cyclic Redundancy Check |
| CSMA/CD | Carrier Sense Multiple Access/Collision Detection |
| CTL3 | Cut Through Layer 3 |
| DHCP | Dynamic Host Control Protocol |
| DGB | Dirección General de Bibliotecas |
| DGSCA | Dirección General de Servicios de Cómputo Académico |
| DSL | Digital Subscriber Line |
| EIA | Electronic Industries Alliance |
| FDDI | Fiber Distributed Data Interface |
| FTP | File Transfer Protocol |
| FX | Fiber Wavelength |
| HTTP | Hypertext Transfer Protocol |
| ICMP | Internet Control Message Protocol |
| ICANN | Internet Corporation for Assigned Names and Numbers |
| IDF | Intermediate Distribution Frame |
| IDM | Intelligent Database Machine |
| IEEE | Institute of Electrical and Electronics Engineers |
| IGMP | Internet Group Management Protocol |
| IP | Internet Protocol |
| ISN | Initial Sequence Number |
| ISO | International Standard Organization |
| ISP | Internet Service Provider |
| GAN | Global Area Network |
| Gbps. | Gigabits por segundo |
| LAN | Local Area Network |
| LH | Long Haul |
| LLC | Logical Link Control |
| LR | Long Range |
| LX | Long Wavelength |
| MAC | Media Access Control |
| MAN | Metropolitan Area Network |
| Mbps | Megabits por segundo |
| MDF | Main Distribution Frame |
| NAT | Network Address Translation |
| NIC | Network Interface Card |
| OSI | Open System Interconexion |

| | |
|---|---|
| OSPF | Open Short Path First |
| PAN | Personal Area Network |
| PCI | Peripheral Component Interconnect |
| POP3 | Post Office Protocol Version 3 |
| PPL3 | Packet by Packet Layer 3 |
| PSTN | Public Switched Telephone Net |
| RARP | Reverse Address Resolution Protocol |
| RIP | Routing Information Protocol |
| RIU | Red Inalámbrica Universitaria |
| SMTP | Simple Mail Transfer Protocol |
| SOHO | Small Office, Home Office |
| SR | Short Range |
| SX | Short Wavelength |
| TIA | Telecommunications Industry Association |
| TCP | Transmission Control Protocol |
| UDP | User Datagram Protocol |
| UPS | Uninterrupted Power System |
| UTP | Unshielded Twisted Pair |
| VLAN | Virtual Local Area Network |
| WAN | Wide Area Network |
| WPAN | Wireless Personal Area Network |
| WIMAX | Worldwide Interoperability for Microwave Access |
| WLAN | Wireless Local Area Network |
| ZX | Extended Distance |

# REFERENCIAS

[1] Barrera González, Pastor. “Conceptos básicos para la comunicación por medio de la fibra óptica”. Monografía de Licenciatura. Escuela Superior de Ingeniería Mecánica, IPN. México, D.F. 1991. Págs. 35-44.

[2] Contreras Barrera, Marcial. “Diseño e instalación de una red LAN bajo el ambiente Unix para la Dirección General de Bibliotecas”. Tesis de Licenciatura. Facultad de Ingeniería, UNAM. México, D.F. 1996. Págs. 9-17, 20-49.

[3] Enríquez Castro, Laura Sonia y Rodrigo Ramírez López. “Implementación de una red inalámbrica en la Biblioteca Central”. Tesis de Licenciatura. Facultad de Ingeniería, UNAM. México, D.F. 2009. Págs. 1-6, 13-23, 40-44, 68-73.

[4] Gamero Arenas, Arcadio. “Implementación de un sistema de cableado estructurado para la modernización de la red de comunicaciones de la DGB de la UNAM”. Tesis de Licenciatura. FES Aragón, UNAM. Estado de México. 2005. Págs. 13-125.

[5] García Anaya, Liz Marlene. “Sistema de Administración de redes locales y de área amplia para un centro de control de energía”. Tesis de Licenciatura. Facultad de Ingeniería, UNAM. México, D.F. 2003. Págs. 7-35

[6] Mateos Muñoz, Agustín. “Ejercicios ortográficos”. 52ª edición. Editorial Esfinge. México, D.F. 2004. Págs. 9-268.

[7] McLen, Ian. “La biblia de TCP/IP”. Editorial Anaya Multimedia. México, D.F. 2001. Págs. 57-59, 80-94, 151-160, 181-203, 233-259, 321-328, 360-362.

[8] Tanenbaum, Andrew S. “Redes de computadoras”. 4ª edición. Editorial Pearson Educación de México. México, D.F. 2003. Págs. 12-24, 37-48, 85-99, 183-199, 247-273, 343-347, 431-458, 532-540, 579-589, 776-778.

[9] Vigueras Villaseñor, Marco Antonio. “Apuntes de la materia de Redes de Computadoras”. Facultad de Ingeniería, UNAM. México, D.F. 2002. Págs. 2-26, 47-60.

[10] “Conceptos básicos de IPv4”. 2010. Págs. 2-20.

[11] “Conceptos básicos de LAN Switching”. 2010. Págs. 3- 31.

[12] “Dell Precision Workstation 370 Manual del propietario”. 2005. Págs. 69-148.

[13] "Memoria Técnica". Infraestructura de red LAN BC. México, D.F. 2007.

[14] "OpenBSD 3.3 y Puente del área de consulta electrónica (Instalación de OpenBSD, Creación de Puente, Activación de PF y Definición de Políticas)". 2003.

[15] "OpenBSD 4.7 Installation Guide". 2009.

[16] "PF: The OpenBSD Packet Filter". 2010.

[17] "Seminario de Conectividad Avanzada". 2001. Págs. 6-20.

[18] "Temas avanzados de IPv4". 2010. Págs. 2-19.

[19] http://bc.unam.mx/historia.html Historia de la Biblioteca Central de la UNAM. 03-septiembre-2010.

[20] http://dgb.unam.mx Sitio de la página web de la Dirección General de Bibliotecas. 03-septiembre-2010.

[21] http://es.wikipedia.org/wiki/Firewall_(informática) Artículo sobre el uso y características del firewall. 03-septiembre-2010.

[22] http://fmc.axarnet.es/redes/indice_m.htm Tutorial referente a la teoría de redes y comunicaciones. 03-septiembre-2010.

[23] http://gabymoonligth.blogspot.es/tags/switch Artículo referente al switch. 03-septiembre-2010.

[24] http://neutron.ing.ucv.ve/revista-e/No4/articulo.htm Artículo sobre la comparación del switcheo y el ruteo. 03-septiembre-2010.

[25] http://standards.ieee.org/getieee802 Sitio oficial de IEEE, donde se puede encontrar documentación referente a las normas IEEE802. 03-septiembre-2010.

[26] http://www.csae.map.es/csi/silice/Redaremet2.html Manual sobre la red MAN del Consejo Superior de Administración Electrónica, España. 03-septiembre-2010.

[27] http://www.extremenetworks.com/Resources/Default.aspx?q=ug Página con documentación técnica de los switches extreme networks. 03-septiembre-2010.

[28] http://www.ietf.org/rfc.html Sitio web oficial del grupo Internet Engineering Task Force, la cual realiza los Request For Comments. 03-septiembre-2010.

[29] http://www.tiaonline.org Sitio web oficial del grupo Telecommunications Industry Association, dedicado a los estándares TIA para el cableado estructurado. 03-septiembre-2010.

[30] http://www.openbsd.org Sitio oficial de OpenBSD.

[31] http://www.tress.com.mx/boletin/julio2003/firewall.htm Artículo sobre el firewall, qué es y para qué sirve. 03-septiembre-2010.

[32] http://www.3com.com/services/resources.html Soporte y documentación técnica de switches 3com. 03-septiembre-2010.

[33] http://132.248.9.181/soporte/index.php Página web de la DGB para el control de inventarios.